PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-022216
(43)Date of publication of application : 24.01.2003

(51)Int.CI. G06F 12/14
B42D 15/10
G06K 19/07

(21)Application number : 2001-207210
(22)Date of filing : 09.07.2001

(71)Applicant : HITACHI LTD
(72)Inventor : HATANO TOMIHISA
TODA AKINORI
TSUNODA MOTOYASU
MIZUSHIMA EIGA
KATAYAMA KUNIHIRO

(54) STORAGE DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To realize the high speed processing of a multi-media card.
SOLUTION: This storage device is provided with a flash memory chip 130, an IC card chip 150 capable of executing security processing (encryption or decoding or the like), and a controller chip 120 for controlling the reading/ writing of data for the flash memory chip and the IC card chip. Moreover, the controller chip 120 simultaneously accesses the flash memory chip 130 and the IC chard chip 150 in response to a request from a host.

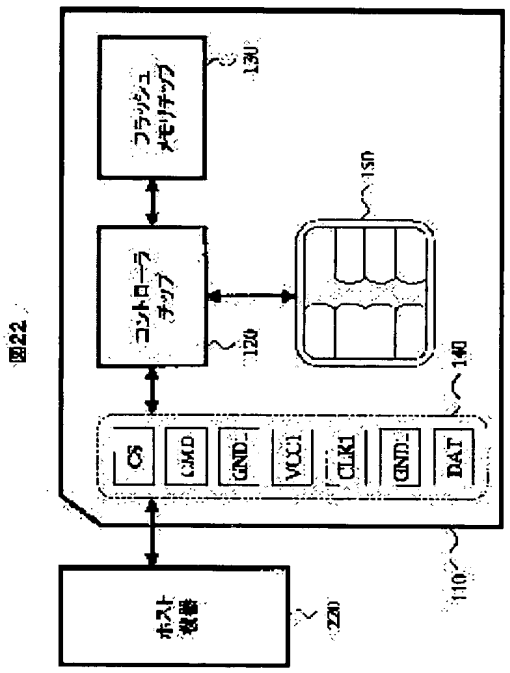


図22

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－22216
（Ｐ２００３－２２２１６Ａ）
(43)公開日　平成15年１月24日(2003.1.24)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
G06F 12/14	320	G06F 12/14	320	B 2C005
	310		310	K 5B017
B42D 15/10	501	B42D 15/10	501	B 5B035
	521		521	
G06K 19/07		G06K 19/00	N	

審査請求　未請求　請求項の数８　ＯＬ　（全36頁）

(21)出願番号　特願2001－207210(Ｐ2001－207210)

(22)出願日　平成13年７月９日(2001.7.9)

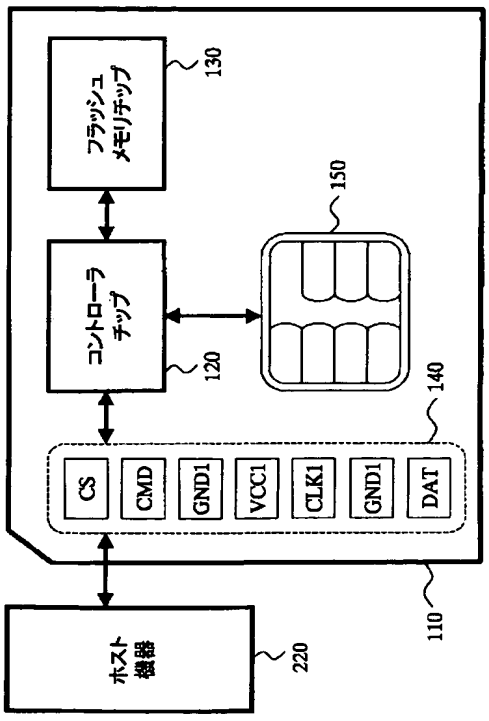
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　幡野　富久
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　戸田　昭憲
神奈川県横浜市戸塚区吉田町292番地　株式会社日立マイクロソフトウェアシステムズ内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】記憶装置

(57)【要約】
【課題】本発明は、マルチメディアカードの処理の高速化を図ることを目的とする。
【解決手段】本発明は、フラッシュメモリチップ１３０と、セキュリティ処理（暗号化や復号化等）を実行可能なＩＣカードチップ１５０と、ホストからの要求に応じて、フラッシュメモリチップ及びＩＣカードチップへのデータの読み書きを制御するコントローラチップ１２０とを備える。さらに、コントローラチップ１２０は、フラッシュメモリチップ１３０とＩＣカードチップ１５０の両方にホストからの要求に応じて同時にアクセスする。

図22



1

【特許請求の範囲】

【請求項１】データを記憶するための記憶装置において、前記データを記憶可能な第１のメモリと、
前記データを記憶可能でかつ前記データのセキュリティ処理を実行可能な第２のメモリと、
ホスト機器からのコマンドに基づいて、前記第１のメモリ又は前記第２のメモリを選択するコントローラとを有し、
前記ホスト機器から前記第１のメモリへのアクセスを実行している間に前記第２のメモリに対する前記ホスト機器からの第２のコマンドを受け付け、前記第２のコマンドに従う処理を実行することを特徴とする記憶装置。

【請求項２】前記コントローラは、前記ホスト機器からのコマンドに前記データのセキュリティ処理に関する情報が含まれていた場合に、前記第２のメモリを選択する請求項１に記載の記憶装置。

【請求項３】前記第２のメモリは、セキュリティ評価機関によって予め認証されたＩＣチップであることを特徴とする請求項１記載の記憶装置。

【請求項４】前記認証済ＩＣチップは、該認証済ＩＣチップへ読み書きされるデータを暗号化又は復号化する手段を有することを特徴とする請求項３記載の記憶装置。

【請求項５】前記第１のメモリは、前記ホスト機器からのデータを記憶する第１の記憶領域と、前記第２のメモリに関するデータを記憶し、前記ホスト機器からのデータの読み出し又は書き込みの少なくとも１つが制限される第２の記憶領域とを有することを特徴とする請求項４記載の記憶装置。

【請求項６】前記コントローラは、前記第２の記憶領域に記憶されたデータを、前記第２のメモリへ転送する手段を有することを特徴とする請求項５記載の記憶装置。

【請求項７】前記コントローラは、前記第２の記憶領域に記憶されたデータに基づいて、前記第２のメモリを制御することを特徴とする請求項６記載の記憶装置。

【請求項８】コンテンツプロバイダによって発行されたセッション鍵によって暗号化された第一及び第二のコンテンツを記憶するメモリと、
前記コンテンツプロバイダによって公開鍵によって暗号化されたセッション鍵と前記公開鍵に対応する秘密鍵とを記憶し、前記秘密鍵によって前記セッション鍵を復号化することが可能なメモリ付演算処理装置と、
ホストからのコマンドに応じて、前記メモリ付演算処理装置に前記第一のコンテンツに対応する前記セッション鍵の復号化させながら、既に復号化された前記第二のコンテンツに対応する前記セッション鍵によって前記メモリに記憶された前記第二のコンテンツを復号化し、復号化された前記コンテンツを前記ホストへ送信するコントローラとを備えた記憶装置。

【発明の詳細な説明】

【０００１】

2

【発明の属する技術分野】本発明は、セキュリティ機能を搭載した記憶装置、その記憶装置が挿入可能なホスト機器、及びその記憶装置が挿入されたホスト機器に係り、特に、フラッシュメモリチップ及びコントローラを有するメモリカード及びそのメモリカードが挿入可能な装置及びそのそのメモリカードが挿入された端末装置に関する。

【０００２】

【従来の技術】ＩＣカードは、プラスチックカード基板中にＩＣ（集積回路）チップを埋め込んだものであり、その表面にＩＣチップの外部端子を持つ。ＩＣチップの外部端子には、電源端子、クロック端子、データ入出力端子などが含まれる。ＩＣチップは、接続装置が外部端子から電源や駆動クロックを直接供給することによって動作する。

【０００３】ＩＣカードは、外部端子を通して端末機などの接続装置との間で電気信号を送受信することにより、接続装置と情報交換をおこなう。情報交換の結果として、ＩＣカードは計算結果や記憶情報の送出、記憶情報の変更をおこなう。ＩＣカードは、これらの動作仕様に基づいて、機密データ保護や個人認証などのセキュリティ処理を実行する機能を持つことができる。ＩＣカードは、クレジット決済やバンキングなど機密情報のセキュリティが必要とされるシステムにおいて、個人識別のためのユーザデバイスとして利用されている。

【０００４】

【発明が解決しようとする課題】セキュリティシステムにおいて利用されるＩＣカードは、ＩＣカード内部で秘密情報を用いて演算を行う際に、その秘密情報あるいはその秘密情報を推定できるような情報をＩＣカードの外部にもらさないように設計される必要がある。すなわち、耐タンパ性を持つことが必要とされる。このような外部にもらしてはならない秘密情報を解析する攻撃方法としては、タイミング解析、電力差分解析、故障利用解析などが知られている。

【０００５】タイミング解析は、暗号処理時間が秘密情報の内容に依存して異なる場合、その時間差を統計的に解析して秘密情報を推定する攻撃法である。暗号アルゴリズムを装置に実装する際、暗号の処理時間の短縮やプログラムサイズの縮小を目的として、秘密情報の内容に依存して不要となる処理をスキップしたり分岐処理を行ったりするような最適化が行われることがある。このような最適化を行った場合、暗号処理時間が秘密情報の内容に依存して異なる。そのため、処理時間を見ることで秘密情報の内容を推定できる可能性がある。

【０００６】電力差分解析は、暗号処理を実行している最中に、ＩＣカードの電源端子から供給される電力を測定し、そこから消費電力の差分を解析することにより秘密情報を推定する攻撃法である。

【０００７】故障利用解析は、ＩＣカードの計算誤りを

利用した攻撃法である。ＩＣカードに一過性の故障あるいは他の機能に影響を与えない範囲の限定的な障害を与え、ＩＣカードに攻撃者の望む異常な処理を行わせる。例えば、ＩＣカードに高電圧を加えたり、瞬間的にクロック周波数や駆動電圧を変動させることにより故意にエラーを発生させた場合に得られる誤った計算結果と正しい計算結果から秘密情報が取得される可能性がある。

【０００８】したがって、ＩＣカードは、実用上、これらの攻撃法に対する対策手段を持たなければならない。

【０００９】本発明の目的は、セキュリティを向上した記憶装置を提供することにある。

【００１０】

【課題を解決するための手段】上記課題を解決するため、本発明は、データを記憶するための記憶装置において、データを記憶可能な第１のメモリと、データを記憶可能でかつデータのセキュリティ処理を実行可能な第２のメモリと、ホスト機器からのコマンドに基づいて、第１のメモリ又は第２のメモリを選択するコントローラと有し、ホスト機器から第１のメモリへのアクセスを実行している間に第２のメモリに対するホストからの第２のコマンドを受け付け、第２のコマンドに従う処理を実行する構成とする。

【００１１】又、コントローラは、ホスト機器からのコマンドにデータのセキュリティ処理に関する情報が含まれていた場合に、第２のメモリを選択する構成でも良い。

【００１２】さらに、第２のメモリは、セキュリティ評価機関によって予め認証されたＩＣチップであることも考えられる。

【００１３】また、認証済ＩＣチップは、認証済ＩＣチップへ読み書きされるデータを暗号化又は復号化する手段を有する。

【００１４】また、第１のメモリは、ホスト機器からのデータを記憶する第１の記憶領域と、第２のメモリに関するデータを記憶し、ホスト機器からのデータの読み出し又は書き込みの少なくとも１つが制限される第２の記憶領域とを有する構成とすることもできる。

【００１５】さらに、コントローラは、第２の記憶領域に記憶されたデータを、第２のメモリへ転送する手段を有することもできる。

【００１６】また、コントローラは、第２の記憶領域に記憶されたデータに基づいて、第２のメモリを制御する構成を有しても良い。

【００１７】さらに、本発明の実施形態として、コンテンツプロバイダによって発行されたセッション鍵によって暗号化された第一及び第二のコンテンツを記憶するメモリと、コンテンツプロバイダによって公開鍵によって暗号化されたセッション鍵と公開鍵に対応する秘密鍵とを記憶し、秘密鍵によってセッション鍵を復号化することが可能なメモリ付演算処理装置と、ホスト機器からのコマンドに応じて、メモリ付演算処理装置に第一のコンテンツに対応するセッション鍵の復号化させながら、既に復号化された第二のコンテンツに対応するセッション鍵によってメモリに記憶された第二のコンテンツを復号化し、復号化された第二のコンテンツをホスト機器へ送信するコントローラとを有する構成とする。

【００１８】

【発明の実施の形態】図２２は、本発明を適用したＭｕｌｔｉＭｅｄｉａＣａｒｄ（ＭｕｌｔｉＭｅｄｉａＣａｒｄは、ＩｎｆｉｎｅｏｎＴｅｃｈｎｏｌｏｇｉｅｓＡＧの登録商標である。以下、「ＭＭＣ」と略記する。）の内部構成を示した図である。ＭＭＣ１１０は、ＭＭＣ仕様に準拠するのが好ましい。ＭＭＣ１１０は、ＭＭＣ１１０に接続されたホスト機器２２０から発行されたＭＭＣ仕様に準拠したメモリカードコマンドに基づいて、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。

【００１９】ホスト機器２２０は、例えば、携帯電話、携帯情報端末（ＰＤＡ）、パーソナルコンピュータ、音楽再生（及び録音）装置、カメラ、ビデオカメラ、自動預金預払器、街角端末、及び決済端末等が該当する。

【００２０】ＭＭＣ１１０は、ＭＭＣ外部端子１４０、コントローラチップ１２０、フラッシュメモリチップ１３０、及びＩＣカードチップ１５０を持つ。フラッシュメモリチップ１３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。ＭＭＣ外部端子１４０は、外部のホスト機器２２０と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子等の７つの端子から構成される。コントローラチップ１２０は、ＭＭＣ外部端子１４０、フラッシュメモリチップ１３０、及びＩＣカードチップ１５０と接続され、これらを制御するマイコンチップである。

【００２１】ＩＣカードチップ１５０は、ＩＣカードのプラスチック基板中に埋め込むためのマイコンチップであり、ＩＣカードチップ１５０が有する外部端子、電気信号プロトコル、コマンドはＩＳＯ／ＩＥＣ７８１６規格に準拠している。ＩＣカードチップ１５０の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子、及びグランド端子がある。コントローラチップ１２０は、ＩＣカードチップ１５０の外部端子からＩＣカードチップ１５０にＩＣカードコマンドを発行することによって、外部のホスト機器２２０から要求されたセキュリティ処理に必要な演算をおこなう。

【００２２】図２６は、本発明のＩＣカードチップの内部構成を示す図である。ＩＣカードチップ１５０は、演算処理を行うためのＣＰＵ（マイコン）１５８、データ（プログラムを含む。）を記憶するためのＲＯＭ（Read

Only Memory）１５９、ＲＡＭ（Random Access Memory）１６０、ＥＥＰＲＯＭ（Electrically Erasable Programmable ROM）１６２、暗号／復号に間する処理を行うための暗号コプロセッサ１６３、及び外部とデータを送受信するためのシリアルインターフェース１６１とを備える。これらはバス１６４によって相互に接続される。

【００２３】暗号コプロセッサ１６３は、ホスト機器２２０からのコマンドに応じて、、セキュリティ処理を実行する。尚、暗号コプロセッサ１６３（ハードウェア）の替わりに、プログラム（ソフトウェア）を用いてＣＰＵ１５８がセキュリティ処理を実行してもよい。セキュリティ処理は、例えば、ＩＣカードチップ１５０内の記憶領域にデータが書き込まれるとき、又は、ＩＣカードチップ１５０内の記憶領域からデータが読み出されるときに実行される。

【００２４】フラッシュメモリチップ１３０は、不揮発性の記憶素子を有する。一般的に、ＩＣカードチップ１５０のＥＥＰＲＯＭ１６２の記憶容量は、フラッシュメモリチップ１３０の記憶容量より小さい。但し、ＥＥＰＲＯＭ１６２の記憶容量は、フラッシュメモリチップ１３０の記憶容量と同じでもよいし、大きくてもよい。

【００２５】ＩＣカードチップ１５０には、セキュリティ評価基準の国際標準であるＩＳＯ／ＩＥＣ１５４０８の評価・認証機関によって認証済みである製品を利用するのが望ましい。一般に、セキュリティ処理をおこなう機能を持つＩＣカードを実際の電子決済サービスなどで利用する場合、そのＩＣカードはＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。ＭＭＣにセキュリティ処理をおこなう機能を追加することによってＭＭＣ１１０を実現し、それを実際の電子決済サービスなどで利用する場合、ＭＭＣ１１０も同様にＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。本発明においては、ＭＭＣ１１０は、評価・認証機関によって認証済みのＩＣカードチップ１５０を内蔵し、そのＩＣカードチップ１５０を利用してセキュリティ処理をおこなう構造を持つことにより、セキュリティ処理機能を得る。したがって、ＭＭＣ１１０はＩＳＯ／ＩＥＣ１５４０８に基づくセキュリティ評価基準を容易に満足することができ、ＭＭＣにセキュリティ処理機能を追加するための開発期間を短縮することができる。

【００２６】ＭＭＣ１１０は、ＭＭＣ仕様に準拠した外部インタフェースを持つのが好ましい。ＭＭＣ１１０は、一種類の外部インタフェースを通じて、標準メモリカードコマンド（フラッシュメモリチップ１３０へアクセスするためのコマンド）に加えて、セキュリティ処理を実行するコマンドを受け付ける必要がある。コントローラチップ１２０は、ＭＭＣ１１０が受信したコマンドが標準メモリカードコマンドであるか、セキュリティ処理を実行するコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。本実施形態においては、コントローラチップ１２０は、標準メモリカードコマンドを受信したならば、フラッシュメモリチップ１３０を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュリティ処理を実行するコマンドを受信したならば、ＩＣカードチップ１５０を選択し、これにＩＣカードコマンドを発行してセキュリティ処理を実行することができる。

【００２７】ＩＣカードチップ１５０の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子がコントローラチップ１２０と接続されている。

【００２８】コントローラチップ１２０は、電源供給端子、クロック入力端子を通して、ＩＣカードチップ１５０への電源供給、クロック供給を制御する。本実施形態によれば、ホスト機器２２０からセキュリティ処理を要求されないときには、コントローラチップ１２０がＩＣカードチップ１５０への電源供給やクロック供給を停止することができ、ＭＭＣ１１０の電力消費を削減することができる。

【００２９】電源が供給されていないＩＣカードチップ１５０を、ＩＣカードコマンドを受信できる状態にするには、まず、ＩＣカードチップ１５０に電源供給を開始し、リセット処理を施す必要がある。コントローラチップ１２０は、ＭＭＣ１１０がホスト機器２２０からセキュリティ処理を実行するコマンドを受信したのを契機に、電源供給端子を通してＩＣカードチップ１５０への電源供給を開始する機能を有する。また、コントローラチップ１２０は、ＭＭＣ１１０がホスト機器２２０からセキュリティ処理を実行するコマンドを受信したのを契機に、リセット入力端子を通してＩＣカードチップ１５０のリセット処理をおこなう機能を有する。本実施形態によれば、コントローラチップ１２０は、セキュリティ処理を実行するコマンドを受信するまでＩＣカードチップ１５０への電源供給を停止させておくことができる。したがって、ＭＭＣ１１０の電力消費を削減することができる。

【００３０】コントローラチップ１２０は、ＩＣカードチップ１５０のクロック入力端子を通してＩＣカードチップ１５０に供給するクロック信号をＭＭＣ１１０内部で発生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を有する。本実施形態によれば、ＭＭＣ外部端子１４０のクロック入力端子のクロック信号と無関係にすることができるため、ホスト機器２２０によるタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。

【００３１】図２１は、フラッシュメモリチップ１３０の内部構成を示す図である。フラッシュメモリチップ１

３０は、ホストデータ領域２１１５及び管理領域２１１０とを有する。ホストデータ領域２１１５は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器２２０が論理アドレスを指定してデータを読み書きできる領域である。

【００３２】ホストデータ領域２１１５は、ユーザファイル領域２１３０及びセキュリティ処理アプリケーション領域２１２０とを有する。ユーザファイル領域２１３０は、ユーザが自由にファイルデータを読み書きできる領域である。セキュリティ処理アプリケーション領域２１２０は、ホスト機器２２０がセキュリティ処理アプリケーションに必要なデータを格納する領域であり、ユーザが不正にアクセスしないように、ホスト機器２２０のセキュリティ処理アプリケーションによって論理的にユーザアクセス制限がかけられる。ここに格納されるデータとしては、ホスト機器２２０のアプリケーションプログラム、そのアプリケーション専用のデータ、及びセキュリティ処理に使用される証明書など（例えば、電子決済アプリケーションプログラム、電子決済ログ情報、電子決済サービス証明書など）がある。本実施形態によれば、ＭＭＣ１１０が、ホスト機器２２０がセキュリティ処理をおこなう上で使用するデータをホスト機器２２０の代わりに格納するため、ホスト機器２２０にとって利便性が向上する。

【００３３】管理領域２１１０は、コントローラチップ１２０がＩＣカードチップ１５０を管理するための情報を格納する領域である。管理領域２１１０は、ＩＣカード制御パラメータ領域２１１１、ＩＣカード環境設定情報領域２１１２、ＣＬＫ２設定情報領域２１１３、セキュリティ処理バッファ領域２１１４、及びセキュリティ処理ステータス領域２１１６とを有する。２１１１～２１１６の領域の詳細な使用法については後述する。

【００３４】コントローラチップ１２０は、フラッシュメモリチップ１３０の管理領域２１１０のセキュリティ処理バッファ領域２１１４を、ＩＣカードチップ１５０でセキュリティ処理を実行する際のメインメモリまたはバッファメモリとして利用する。ホスト機器２２０がセキュリティ処理を実行するコマンドによりＭＭＣ１１０にアクセスした際に、ＭＭＣ１１０がホスト機器２２０からＩＣカードチップ１５０に一度に送信できないほどの大きなサイズのセキュリティ関連データを受信したならば、コントローラチップ１２０は、フラッシュメモリチップ１３０へのアクセスを選択し、受信したデータを十分な容量を持つセキュリティ処理バッファ領域２１１４に一時的に格納する。ＩＣカードチップ１５０に一度に送信できないほどのサイズとは、ＩＣカードコマンドの許容データサイズ（例えば、２５５バイト又は２５６バイト）を超えるサイズである。そして、コントローラチップ１２０はそれをＩＣカードチップ１５０に送信できるサイズのデータに分割し、分割データをフラッシュメモリチップ１３０から読み出し、段階的にＩＣカードチップ１５０に送信する。つまり、分割されたデータの読み出し、書き込みを繰り返す。本実施形態によれば、ホスト機器２２０にとって、大きなサイズのセキュリティ関連データを扱うことができるので、セキュリティ処理の利便性が向上する。

【００３５】セキュリティ処理バッファ領域２１１４を含む管理領域２１１０は、ホスト機器２２０が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ１２０により物理的にホストアクセス制限がかけられている。つまり、管理領域２１１０はホスト機器２２０が直接データを読み書きできない。本実施形態によれば、ホスト機器２２０がセキュリティ処理バッファ領域２１１４の内容を自由に読み出したり改ざんすることができないため、セキュリティ処理の信頼性や安全性が向上する。

【００３６】図２３は、ＭＭＣ１１０を利用したセキュリティ処理の一例として、コンテンツ配信のセキュリティ処理を表した図である。コンテンツプロバイダ２３１０は、ＭＭＣ１１０を所有するユーザにコンテンツ２３１４を販売する業者である。ホスト機器２２０は、この例では、コンテンツプロバイダ２３１０とネットワークなどを介して接続することができる端末機である。ユーザは、ＭＭＣ１１０をホスト機器２２０に接続してコンテンツ２３１４を購入する。以下、その手順を説明する。

【００３７】まず、ホスト機器２２０は、ＭＭＣ１１０に、フラッシュメモリチップ１３０に格納されたユーザ証明書２３２１を読み出すコマンドを発行する。ＭＭＣ１１０のコントローラチップ１２０は、フラッシュメモリチップ１３０のセキュリティ処理アプリケーション領域２１２０に格納されたユーザ証明書２３２１を読み出し、それをホスト機器２２０に送信する。ユーザ証明書２３２１を受信したホスト機器２２０は、それをコンテンツプロバイダ２３１０に送信する。コンテンツプロバイダ２３１０は、ユーザ証明書２３２１につけられたデジタル署名を検証する（２３１１）。検証が成功したならば、コンテンツプロバイダ２３１０は、乱数発生器によりセッション鍵を生成し（２３１２）、それをユーザ証明書２３２１から抽出したユーザ公開鍵によって暗号化する（２３１３）。さらに、コンテンツプロバイダ２３１０は、コンテンツ２３１４をセッション鍵によって暗号化する（２３１５）。コンテンツプロバイダ２３１０は、ステップ２３１３の結果をホスト機器２２０に送信する。

【００３８】ホスト機器２２０は、ステップ２３１３の結果をユーザ秘密鍵２３２２によって復号するセキュリティ処理を要求するコマンドを、ＭＭＣ１１０に発行する。コントローラチップ１２０は、ステップ２３１３の結果をユーザ秘密鍵２３２２によって復号するＩＣカー

ドコマンドを、ＩＣカードチップ１５０に発行する。ＩＣカードチップ１５０は、ユーザ秘密鍵２３２２によってステップ２３１３の結果を復号して、セッション鍵を取得する（２３２３）。ホスト機器２２０は、この復号処理が成功したかを示す情報を出力させるコマンドをＭＭＣ１１０に発行する。コントローラチップ１２０は、ＩＣカードチップ１５０の出力する復号結果（復号処理が成功したかを示すＩＣカードレスポンス）をもとにしてホスト機器２２０の求める情報を構築する。そして、ＭＭＣ１１０はその情報をホスト機器２２０に送信する。

【００３９】次に、コンテンツプロバイダ２３１０は、ステップ２３１５の結果を、ホスト機器２２０に送信する。ホスト機器２２０は、ステップ２３１３の結果をセッション鍵（ステップ２３２３によって取得した鍵）によって復号するセキュリティ処理を要求するコマンドを、ＭＭＣ１１０に発行する。コントローラチップ１２０は、ステップ２３１５の結果をセッション鍵によって復号するＩＣカードコマンドを、ＩＣカードチップ１５０に発行する。ＩＣカードチップ１５０は、セッション鍵によってステップ２３１５の結果を復号して、コンテンツ２３１４を復元する（２３２４）。コントローラチップ１２０は、このコンテンツ２３１４をＩＣカードチップ１５０から受信し、フラッシュメモリチップ１３０に書きこむ。ホスト機器２２０は、この復号処理が成功したかを示す情報を出力させるコマンドをＭＭＣ１１０に発行する。コントローラチップ１２０は、ＩＣカードチップ１５０の出力する復号結果（復号処理が成功したかを示すＩＣカードレスポンス）をもとにしてホスト機器２２０の求める情報を構築する。そして、ＭＭＣ１１０はその情報をホスト機器２２０に送信する。ホスト機器２２０が、コンテンツを無事に受信したことをコンテンツプロバイダ２３１０に伝えると、コンテンツプロバイダ２３１０はユーザ証明書に記載されたユーザにコンテンツ料金を課金する。ユーザは、ホスト機器２２０でＭＭＣ１１０内のフラッシュメモリチップ１３０に格納されたコンテンツ２３１４を読み出して利用することができる。また、フラッシュメモリチップ１３０の記憶媒体に大容量のフラッシュメモリを使用すれば、多くのコンテンツを購入できる。本実施形態によれば、コンテンツ配信におけるセキュリティ処理とコンテンツ蓄積の両方をＭＭＣ１１０によって容易に実現できる。コンテンツ料金の決済を、ＩＣカードチップ１５０を利用して行ってもよい。

【００４０】図２４及び図２５は、それぞれ、本発明をＳＤカード（幅２４ミリメートル、長さ３２ミリメートル、厚さ２。１ミリメートルで、９つの外部端子をもち、フラッシュメモリを搭載した小型メモリカードである。）及びメモリースティック（メモリースティックはソニー株式会社の登録商標である。）に適用したときの内部構成を表した図である。

【００４１】本発明を適用したＳＤカード２４１０は、ＳＤカードコントローラチップ２４２０、フラッシュメモリチップ２４３０、ＳＤカード外部端子２４４０、及びＩＣカードチップ１５０とを有する。本発明を適用したメモリースティック２５１０は、メモリースティックコントローラチップ２５２０、フラッシュメモリチップ２５３０、メモリースティック外部端子２５４０、及びＩＣカードチップ１５０とを有する。

【００４２】フラッシュメモリチップ２４３０及び２５３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。ＳＤカードコントローラチップ２４２０及びメモリースティックコントローラチップ２５２０は、それぞれＳＤカードとメモリースティック内の他の構成要素を制御するマイコンチップである。

【００４３】ＳＤカード外部端子２４４０は、端からＤａｔａ２端子２４４１、Ｄａｔａ３端子２４４２、Ｃｏｍ端子２４４３、Ｖｓｓ端子２４４４、Ｖｄｄ端子２４４５、Ｃｌｏｃｋ端子２４４６、Ｖｓｓ端子２４４７、Ｄａｔａ０端子２４４８、Ｄａｔａ１端子２４４９の順で並ぶ９つの端子を有する。Ｖｄｄ端子２４４５は電源供給端子、Ｖｓｓ端子２４４４及び２４４７はグランド端子、Ｄａｔａ０端子２４４８、Ｄａｔａ１端子２４４９、Ｄａｔａ２端子２４４１及びＤａｔａ３端子２４４２はデータ入出力端子、Ｃｏｍ端子２４４３はコマンド入出力端子、Ｃｌｏｃｋ端子２４４６はクロック入力端子である。ＳＤカード２４１０は、外部に接続するＳＤカードホスト機器２４６０とのインタフェース仕様がＭＭＣ１１０と異なるものの、ＭＭＣ外部端子１４０と非常に類似した外部端子を持ち、ＭＭＣ１１０と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

【００４４】一方、メモリースティック外部端子２５４０は、端からＧｎｄ端子２５４１、ＢＳ端子２５４２、Ｖｃｃ端子２５４３、予約端子ＲｓｖをＩつ飛ばしてＤＩＯ端子２５４４、ＩＮＳ端子２５４５、予約端子ＲｓｖをＩつ飛ばしてＳＣＫ端子２５４６、Ｖｃｃ端子２５４７、Ｇｎｄ端子２５４８の順で並ぶＩＯ個の端子を有する。Ｖｃｃ端子２５４３及び２５４７は電源供給端子、Ｇｎｄ端子２５４１及び２５４８はグランド端子、ＤＩＯ端子２５４４はコマンドおよびデータ入出力端子、ＳＣＫ端子２５４６はクロック入力端子である。メモリースティック２５１０は、外部に接続するメモリースティックホスト機器２５６０とのインタフェース仕様がＭＭＣ１１０と異なるものの、ＭＭＣ１１０と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

【００４５】図１は、本発明を適用したＭＭＣ１１０の内部構成を表した図である。また、図２は、図１のＭＭ

Ｃ１１０と接続したホスト機器２２０の構成とその接続状態を表した図である。ホスト機器２２０は、ＶＣＣ１電源２２１、ＣＬＫ１発振器２２２、ホストインタフェース２２３を持つ。

【００４６】ＭＭＣ１１０は、外部のホスト機器２２０と情報交換するためのＭＭＣ外部端子１４０を持つ。ＭＭＣ外部端子１４０は、ＣＳ端子１４１、ＣＭＤ端子１４２、ＧＮＤ１端子１４３及び１４６、ＶＣＣ１端子１４４、ＣＬＫ１端子１４５、ＤＡＴ端子１４７の７つの端子を有する。ＭＭＣ仕様は、ＭＭＣ１１０の動作モードとしてＭＭＣモードとＳＰＩモードという２種類を規定しており、動作モードによってＭＭＣ外部端子１４０の使用法は異なる。本実施例ではＭＭＣモードでの動作の場合について詳細に説明する。

【００４７】ＶＣＣ１端子１４４は、ＶＣＣ１電源２２１と接続されており、ホスト機器２２０がＭＭＣ１１０に電力を供給するための電源端子である。ＧＮＤ１端子１４３および１４６は、ＶＣＣ１電源２２１と接続されており、ＭＭＣ１１０の電気的なグランド端子である。ＧＮＤ１端子１４３とＧＮＤ１端子１４６は、ＭＭＣ１１０内部で電気的に短絡されている。

【００４８】ＣＳ端子１４１は、ホストインタフェース２２３に接続されており、ＳＰＩモードの動作において使用される入力端子である。ホスト機器２２０が、ＭＭＣ１１０にＳＰＩモードでアクセスするときには、ＣＳ端子１４１にＬレベルを入力する。ＭＭＣモードの動作では、ＣＳ端子１４１を使用する必要はない。ＣＭＤ端子１４２は、ホストインタフェース２２３に接続されており、ホスト機器２２０が、メモリカードインタフェース仕様に準拠したメモリカードコマンドをＭＭＣ１１０に送信したり、同仕様に準拠したメモリカードレスポンスをＭＭＣ１１０から受信するために使用する入出力端子である。ＤＡＴ端子１４７は、ホストインタフェース２２３に接続されており、ホスト機器２２０が、メモリカードインタフェース仕様に準拠した形式の入力データをＭＭＣ１１０に送信したり、同仕様に準拠した形式の出力データをＭＭＣ１１０から受信するために使用する入出力端子である。

【００４９】ＣＬＫ１端子１４５は、ＣＬＫ１発振器２２２に接続されており、ＣＬＫ１発振器２２２が生成するクロック信号が入力される端子である。ホスト機器２２０が、ＣＭＤ端子１４２を通してメモリカードコマンド、メモリカードレスポンスを送受信したり、ＤＡＴ端子１４７を通してホストデータを送受信するときに、ＣＬＫ１端子１４５にクロック信号が入力される。ホストインタフェース２２３には、ＣＬＫ１発振器２２２からクロック信号が供給されており、メモリカードコマンド、メモリカードレスポンス、ホストデータは、ＣＬＫ１発振器２２２が生成するクロック信号にビット単位で同期して、ホスト機器２２０とＭＭＣ１１０との間を転送される。

【００５０】ＭＭＣ１１０は、コントローラチップ１２０を持つ。コントローラチップ１２０は、ＣＰＵ１２１、フラッシュメモリＩ／Ｆ制御回路１２２、ＭＭＣＩ／Ｆ制御回路１２３、ＣＬＫ０発振器１２４、ＶＣＣ２生成器１２５、ＶＣＣ２制御回路１２６、ＣＬＫ２制御回路１２７、ＩＣカードＩ／Ｆ制御回路１２８とを有する。これらの構成要素１２１～１２８は、ホスト機器２２０からＶＣＣ１端子１４４やＧＮＤ１端子１４３、１４６を通して供給された電力により動作する。ＭＭＣＩ／Ｆ制御回路１２３は、ＣＳ端子１４１、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、及びＤＡＴ端子１４７と接続されており、ＭＭＣ１１０がそれらの端子を通してホスト機器２２０と情報交換するためのインタフェースを制御する論理回路である。

【００５１】ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３と接続されており、ＭＭＣＩ／Ｆ制御回路１２３を制御する。ＭＭＣＩ／Ｆ制御回路１２３がＣＭＤ端子１４２を通してホスト機器２２０からメモリカードコマンドを受信すると、ＭＭＣＩ／Ｆ制御回路１２３は、そのコマンドの受信が成功したかどうかの結果をホスト機器２２０に伝えるためＣＭＤ端子１４２を通してホスト機器２２０にレスポンスを送信する。ＣＰＵ１２１は、受信したメモリカードコマンドを解釈し、コマンド内容に応じた処理を実行する。また、そのコマンド内容に応じてホスト機器２２０とＤＡＴ端子１４７を通してデータの送受信をおこなう必要がある場合、ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３へのデータの送出、ＭＭＣＩ／Ｆ制御回路１２３からのデータの取得をおこなう。さらに、ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３とホスト機器２２０との間のデータ転送手続きも制御する。例えば、ホスト機器２２０から受信したデータの処理中に、ホスト機器２２０がＭＭＣ１１０への電源供給を停止することがないように、ＣＰＵ１２１はＤＡＴ端子１４７にＬレベルを出力させ、ＭＭＣ１１０がビジー状態であることをホスト機器２２０に伝える。ＣＬＫ０発振器１２４は、ＣＰＵ１２１と接続され、ＣＰＵ１２１を動作させる駆動クロックを供給する。

【００５２】ＭＭＣ１１０は、フラッシュメモリチップ１３０を有する。フラッシュメモリチップ１３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップである。フラッシュメモリチップ１３０は、ホスト機器２２０からＶＣＣ１端子１４４やＧＮＤ１端子１４３、１４６を通して供給された電力により動作する。フラッシュメモリチップ１３０は、外部からのフラッシュメモリコマンドに従って、入力されたデータを不揮発性の半導体メモリに格納するライト機能、また同メモリに格納されたデータを外部に出力するリード機能を持つ。フラッシュメモリＩ／Ｆ制御回路１２２は、フラッシュメモリチップ１３０にフラッシュメモリコマンドを発行した

り、そのコマンドで入出力するデータを転送するための論理回路である。ＣＰＵ１２１は、フラッシュメモリＩ／Ｆ制御回路１２２を制御し、フラッシュメモリチップ１３０にデータのライト機能やリード機能を実行させる。ホスト機器２２０から受信したデータをフラッシュメモリチップ１３０にライトしたり、フラッシュメモリチップ１３０に格納されたデータをホスト機器２２０に送信する必要があるとき、ＣＰＵ１２１は、フラッシュメモリＩ／Ｆ制御回路１２２とＭＭＣＩ／Ｆ制御回路１２３の間のデータ転送を制御する。

【００５３】ＭＭＣ１１０は、ＩＣカードチップ１５０を有する。ＩＣカードチップ１５０は、ＩＣカードの基板中に埋め込むことを目的として設計されたＩＣチップであり、ＩＣカードの外部端子規格に準拠した８つの外部端子を有する。このうち６つの端子は、ＩＣカードの外部端子規格により使用法が割り付けられており、残りの２つは将来のための予備端子である。その６つの端子は、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、ＧＮＤ２端子１５５、ＶＰＰ端子１５６、及びＩ／Ｏ端子１５７である。

【００５４】ＩＣカードチップ１５０のグランド端子は、ＭＭＣ外部端子１４０のGND1（グランド端子）１４６に接続される。ＩＣカードチップ１５０のＶＣＣ２端子（電源入力端子）１５１は、コントローラチップ１２０のＶＣＣ２制御回路１２６に接続される。ＩＣカードチップ１５０のＲＳＴ端子（リセット入力端子）１５２とＩ／Ｏ端子（データ入出力端子）１５７は、コントローラチップ１２０のＩＣカードＩ／Ｆ制御回路１２８に接続される。ＩＣカードチップ１５０のＣＬＫ２端子（クロック入力端子）１５３は、コントローラチップ１２０のＣＬＫ２制御回路１２７に接続される。

【００５５】フラッシュメモリチップ１３０のＶＣＣ端子（電源入力端子）は、ＭＭＣ外部端子１４０のＶＣＣ１１４４に接続される。フラッシュメモリチップ１３０のＶＳＳ端子（グランド端子）は、ＭＭＣ外部端子１４０のGND1１４６に接続される。フラッシュメモリチップ１３０のＩ／Ｏ端子（データ入出力端子）とレディ／ビジー端子とチップイネーブル端子とアウトプットイネーブル端子とライトイネーブル端子とクロック端子とリセット端子とは、コントローラチップ１２０のフラッシュメモリＩＦ制御回路１２２に接続される。

【００５６】ＶＣＣ２端子１５１は、ＩＣカードチップ１５０に電力を供給するための電源端子である。ＶＣＣ２制御回路１２６は、ＭＯＳ－ＦＥＴ素子を用いたスイッチ回路によりＶＣＣ２端子１５１への電力の供給開始と供給停止を制御する回路である。ＶＣＣ２生成器１２５はＶＣＣ２端子１５１に供給する電圧を発生し、それをＶＣＣ２制御回路１２６に供給する。ＩＣカードの電気信号規格は、ＩＣカードの動作クラスとして、クラスＡとクラスＢを規定している。ＶＣＣ２端子１５１に供給する標準電圧は、クラスＡでは５Ｖ、クラスＢでは３Ｖである。本発明はＩＣカードチップ１５０の動作クラスによらず適用できるが、本実施例ではＩＣカードチップ１５０がクラスＢで動作する場合について詳細に説明する。

【００５７】ＶＰＰ端子１５６は、ＩＣカードチップ１５０がクラスＡで動作する時に、内部の不揮発性メモリにデータを書き込んだり消去したりするために使用される可変電圧を供給する端子であり、クラスＢで動作する時には使用しない。ＧＮＤ２端子１５５は、ＩＣカードチップ１５０の電気的なグランド端子であり、ＧＮＤ１端子１４３、１４６と短絡されている。ＶＣＣ２制御回路１２６はＣＰＵ１２１と接続され、ＣＰＵ１２１はＶＣＣ２端子１５１への電力供給の開始と停止を制御することができる。ＩＣカードチップ１５０を使用しないときは、ＣＰＵ１２１はＶＣＣ２端子１５１への電力供給を停止することができる。ＭＭＣ１１０は、ＩＣカードチップ１５０への電力供給を停止することにより、それが消費する電力を節約することができる。ただし、電力供給を停止すると、ＩＣカードチップ１５０の内部状態は、ＩＣカードチップ１５０内部の不揮発性メモリに記憶されたデータを除いて維持されない。

【００５８】ＣＬＫ２端子１５３は、ＩＣカードチップ１５０にクロック信号を入力する端子である。ＣＬＫ２制御回路１２７は、ＣＬＫ２端子１５３にクロックを供給する回路である。ＣＬＫ２制御回路１２７は、ＣＬＫ０発振器１２４から供給されたクロック信号をもとにしてＣＬＫ２端子１５３に供給するクロック信号を生成する。ＣＬＫ２制御回路１２７はＣＰＵ１２１と接続されており、ＣＬＫ２端子１５３へのクロックの供給開始と供給停止をＣＰＵ１２１から制御することができる。ＩＣカードチップ１５０は、自身内部に駆動クロック発振器をもたない。そのため、ＣＬＫ２端子１５３から駆動クロックを供給することによって動作する。ＣＬＫ２制御回路１２７が、ＣＬＫ２端子１５３へのクロック供給を停止すると、ＩＣカードチップ１５０の動作は停止するため、ＩＣカードチップ１５０の消費電力を低下させることができる。この時、ＶＣＣ２端子１５１への電力供給が保たれていれば、ＩＣカードチップ１５０の内部状態は維持される。

【００５９】ここで、ＣＬＫ２端子１５３に供給するクロック信号の周波数をＦ２、ＣＬＫ０発振器１２４から供給されたクロック信号の周波数をＦ０、ＰとＱを正の整数とすると、ＣＬＫ２制御回路１２７は、Ｆ２＝（Ｐ／Ｑ）＊Ｆ０の関係になるようなクロック信号を作成して、これをＣＬＫ２端子１５３に供給する。ＰとＱの値はＣＰＵ１２１により設定できるようになっている。Ｐを大きく設定してＦ２を大きくすると、ＩＣカードチップ１５０の内部処理をより高速に駆動できる。Ｑを大きく設定してＦ２を小さくすると、ＩＣカードチップ１５

０の内部処理はより低速に駆動され、ＩＣカードチップ１５０の消費電力を低下させることができる。ＩＣカードチップ１５０の駆動クロック周波数は、ＩＣカードチップ１５０が正しく動作できるような許容周波数範囲内に設定される必要がある。そのため、ＣＬＫ２制御回路１２７は、Ｆ２の値がその許容周波数範囲を外れるようなＰとＱの値を設定させない特徴を持つ。

【００６０】Ｉ／Ｏ端子１５７は、ＩＣカードチップ１５０にＩＣカードコマンドを入力したり、ＩＣカードチップ１５０がＩＣカードレスポンスを出力するときに使用する入出力端子である。ＩＣカードＩ／Ｆ制御回路１２８は、Ｉ／Ｏ端子１５７と接続されており、Ｉ／Ｏ端子１５７を通してＩＣカードコマンドの信号送信やＩＣカードレスポンスの信号受信をおこなう回路である。ＩＣカードＩ／Ｆ制御回路１２８はＣＰＵ１２１に接続されており、ＣＰＵ１２１は、ＩＣカードＩ／Ｆ制御回路１２８によるＩＣカードコマンドやＩＣカードレスポンスの送受信の手続きを制御したり、送信すべきＩＣカードコマンドデータをＩＣカードＩ／Ｆ制御回路１２８に設定したり、受信したＩＣカードレスポンスをＩＣカードＩ／Ｆ制御回路１２８から取得する。ＩＣカードＩ／Ｆ制御回路１２８にはＣＬＫ２制御回路１２７からクロックが供給されており、ＩＣカードコマンドやＩＣカードレスポンスは、ＣＬＫ２端子１５３に供給するクロック信号にビット単位で同期して、Ｉ／Ｏ端子１５７を通して送受信される。また、ＲＳＴ端子１５２は、ＩＣカードチップ１５０をリセットするときにリセット信号を入力する端子である。ＩＣカードＩ／Ｆ制御回路１２８は、ＲＳＴ端子１５２と接続されており、ＣＰＵ１２１の指示によりＩＣカードチップ１５０にリセット信号を送ることができる。

【００６１】ＩＣカードチップ１５０は、ＩＣカードの電気信号規格やコマンド規格に基づいて情報交換をおこなう。ＩＣカードチップ１５０へのアクセスパターンは４種類であり、図３～図６を用いて各パターンを説明する。図３は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０が非活性状態（電源が遮断されている状態）から起動して内部状態を初期化するプロセス（以下、コールドリセットと呼ぶ）において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表した図である。図４は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０が活性状態（電源が供給されている状態）で内部状態を初期化するプロセス（以下、ウォームリセットと呼ぶ）において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表した図である。図５は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０にＩＣカードコマンドを送信しＩＣカードチップ１５０からＩＣカードレスポンスを受信するプロセスにおいて、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表した図である。図６は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０を非活性状態にするプロセスにおいて、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表した図である。図３～図６において、時間の方向は左から右にとっており、上の行から下の行に向かってＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、破線はそれぞれの信号の基準（Ｌレベル）を表す。

【００６２】図３を参照して、ＩＣカードチップ１５０のコールドリセット操作を説明する。まず、ＩＣカードＩ／Ｆ制御回路１２８は、ＲＳＴ端子１５２をＬレベルにする（３０１）。次に、ＶＣＣ２制御回路１２６は、ＶＣＣ２端子への電源供給を開始する（３０２）。次に、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（３０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚ（プルアップされた状態）にする（３０４）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＨレベルにする（３０５）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるリセット応答の受信を開始する（３０６）。リセット応答の受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（３０７）。これで、コールドリセットの操作が完了する。なお、ステップ３０７は消費電力を低下させるための工夫であり、省略してもよい。

【００６３】図４を参照して、ＩＣカードチップ１５０のウォームリセット操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（４０１）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＬレベルにする（４０２）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚにする（４０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＨレベルにする（４０４）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるリセット応答の受信を開始する（４０５）。リセット応答の受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（４０６）。これで、ウォームリセットの操作が完了する。なお、ステップ４０６は消費電力を低下させるための工夫であり、省略してもよい。

【００６４】図５を参照して、ＩＣカードチップ１５０にＩＣカードコマンドを送信しＩＣカードチップ１５０からＩＣカードレスポンスを受信する操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（５０１）。なお、クロックがすでに供給されている場合、ステップ５０１は不要である。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７にコマンドデータの送信を開始する（５０２）。コマンドデータの送信が終了したら、ＩＣ

カードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚにする（５０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるレスポンスデータの受信を開始する（５０４）。レスポンスデータの受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（５０５）。これで、ＩＣカードコマンド送信とＩＣカードレスポンス受信の操作が完了する。なお、ステップ５０５は、消費電力を低下させるための工夫であり、省略してもよい。

【００６５】図６を参照して、ＩＣカードチップ１５０を非活性化する操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３をLレベルにする（６０１）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をLレベルにする（６０２）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７をLレベルにする（６０３）。最後に、ＶＣＣ２制御回路１２６はＶＣＣ２端子への電源供給を停止する（６０４）。これで、非活性化の操作が完了する。

【００６６】ＩＣカードチップ１５０は、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。ＩＣカードチップ１５０は、ＣＰＵ１２１との間でＩＣカードコマンドやＩＣカードレスポンスの送受信することにより情報交換をおこない、その結果として、計算の結果や記憶されている情報の送出、記憶されている情報の変更などをおこなう。ＣＰＵ１２１は、ＩＣカードチップ１５０を利用してセキュリティ処理を実行することができる。ＭＭＣ１１０がホスト機器２２０から特定のメモリカードコマンドを受信すると、ＣＰＵ１２１はそれを契機として、ＶＣＣ２制御回路１２６を通してＩＣカードチップ１５０への電源供給を制御したり、またはＣＬＫ２制御回路１２７を通してＩＣカードチップ１５０へのクロック供給を制御したり、またはＩＣカードＩ／Ｆ制御回路１２８を通してＩＣカードチップ１５０にＩＣカードコマンドを送信する。これにより、ＣＰＵ１２１は、ＩＣカードチップ１５０を利用して、ホスト機器２２０が要求するセキュリティ処理を実行する。ＣＰＵ１２１は、特定のメモリカードコマンドの受信を契機に、ＩＣカードチップ１５０に対する電源供給制御、クロック供給制御、ＩＣカードコマンド送信、ＩＣカードレスポンス受信を複数組み合わせて操作することによって、セキュリティ処理を実行してもよい。また、ＣＰＵ１２１は、ホスト機器２２０がＭＭＣ１１０へ電源供給を開始したのを契機として、セキュリティ処理を実行してもよい。セキュリティ処理の結果は、ＩＣカードチップ１５０が出力するＩＣカードレスポンスをベースにして構成され、ＭＭＣ１１０内に保持される。ＭＭＣ１１０がホスト機器２２０から特定のメモリカードコマンドを受信すると、ＣＰＵ１２１はそれを契機として、セキュリティ処理の結果をホスト機器２２０に送信する。

【００６７】図７は、ホスト機器２２０がＭＭＣ１１０にアクセスするときのフローチャートを表したものである。まず、ホスト機器２２０はＭＭＣ１１０を活性化するためにＶＣＣ１端子１４４に電源供給を開始する（７０１）。これを契機として、ＭＭＣ１１０は、第１次ＩＣカード初期化処理を実行する（７０２）。第１次ＩＣカード初期化処理の詳細は後述する。次に、ホスト機器２２０はＭＭＣ１１０を初期化するためにＣＭＤ端子１４２を通してＭＭＣ１１０の初期化コマンドを送信する（７０３）。この初期化コマンドはＭＭＣ仕様に準拠したものであり、複数種類ある。ホスト機器２２０は、ＭＭＣ１１０を初期化するために、複数の初期化コマンドを送信する場合がある。ＭＭＣ１１０が初期化コマンドを受信すると、ＭＭＣ１１０はそれを処理する（７０４）。これを契機として、ＭＭＣ１１０は、第２次ＩＣカード初期化処理を実行する（７０５）。第２次ＩＣカード初期化処理の詳細は後述する。

【００６８】ホスト機器２２０は、ＭＭＣ１１０の初期化コマンドに対するメモリカードレスポンスを、ＣＭＤ端子１４２を通して受信し、そのメモリカードレスポンスの内容からＭＭＣ１１０の初期化が完了したかを判定する。未完了ならば、再び初期化コマンドの送信をおこなう（７０３）。ＭＭＣ１１０の初期化が完了したならば、ホスト機器２２０は、ＭＭＣ仕様に準拠した標準メモリカードコマンド（フラッシュメモリチップ１３０へアクセスするためのコマンド）や、上に述べたセキュリティ処理に関連した特定のメモリカードコマンド（ＩＣカードチップ１５０へアクセスするためのコマンド）の送信を待機する状態に移る（７０７）。この待機状態では、ホスト機器２２０は標準メモリカードコマンドを送信することができる（７０８）。ＭＭＣ１１０が標準メモリカードコマンドを受信したら、ＭＭＣ１１０はそれを処理する（７０９）。処理が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。この待機状態では、ホスト機器２２０はセキュリティ処理要求ライトコマンドを送信することもできる（７１０）。セキュリティ処理要求ライトコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの１種であり、ＭＭＣ１１０にセキュリティ処理を実行させるために処理要求を送信するメモリカードコマンドである。

【００６９】ＭＭＣ１１０がセキュリティ処理要求ライトコマンドを受信したら、ＣＰＵ１２１は、要求されたセキュリティ処理の内容を解釈し、セキュリティ処理をＩＣカードコマンドの形式で記述する（７１１）。即ち、ＣＰＵ１２１は、予め定められたルールに従って、ホスト機器２３０からの標準メモリカードコマンドを、ＩＣカードチップ１５０が解釈可能な特定のメモリカードコマンドへ変換する。そして、その結果として得られ

19

たＩＣカードコマンドをＩＣカードチップ１５０に発行するなどして、要求されたセキュリティ処理を実行する（７１２）。処理が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。この待機状態では、ホスト機器２２０はセキュリティ処理結果リードコマンドを送信することもできる（７１３）。セキュリティ処理結果リードコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの１種であり、ＭＭＣ１１０によるセキュリティ処理の実行結果を知るために処理結果を受信するメモリカードコマンドである。

【００７０】ＭＭＣ１１０がセキュリティ処理結果リードコマンドを受信したら、ＣＰＵ１２１は、ＩＣカードチップ１５０から受信したＩＣカードレスポンスをベースに、ホスト機器２２０に送信すべきセキュリティ処理結果を構築する（７１４）。そして、ホスト機器２２０は、ＭＭＣ１１０からセキュリティ処理結果を受信する。受信が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。なお、ステップ７１４は、ステップ７１２の中でおこなってもよい。

【００７１】図７において、ステップ７０２およびステップ７０５で実行する第１次ＩＣカード初期化処理および第２次ＩＣカード初期化処理は、ＭＭＣ１１０内でセキュリティ処理を実行するのに備えて、ＣＰＵ１２１がＩＣカードチップ１５０に対してアクセスする処理である。具体的には、ＩＣカードチップ１５０の活性化や非活性化、ＩＣカードチップ１５０のリセット、ＩＣカードチップ１５０の環境設定を行う。環境設定とは、セキュリティ処理を実行するために必要な情報（例えば、使用可能な暗号アルゴリズムの情報、暗号計算に使用する秘密鍵や公開鍵に関する情報、個人認証に使用する認証データに関する情報など）をＩＣカードチップ１５０から読み出したり、あるいはＩＣカードチップ１５０に書き込んだりすることを意味する。

【００７２】ＩＣカードチップ１５０の環境設定は、ＩＣカードチップ１５０にＩＣカードコマンドをＮ個（Ｎは正の整数）発行することによっておこなう。例えば、セッション鍵が３個必要ならば、ＩＣカードコマンドを３回発行し、セッション鍵が２個必要ならば、ＩＣカードコマンドを２回発行する。Ｎ個のＩＣカードコマンドは、互いに相違するものであってもよいし、同一のものであってもよい。Ｎの値は固定されたものではなく、状況によってさまざまな値となる。以下、環境設定で発行するＩＣカードコマンドを、設定コマンドと呼ぶ。また、この環境設定に基づいてセキュリティ処理を実行するＩＣカードコマンドを、以下、セキュリティコマンドと呼ぶ。セキュリティコマンドの例としては、デジタル署名の計算、デジタル署名の検証、メッセージの暗号化、暗号化メッセージの復号、パスワードによる認証などをおこなうコマンドがある。

20

【００７３】ＣＰＵ１２１は、ＩＣカードチップ１５０の環境設定の内容を自由に変更することができる。ＣＰＵ１２１は、セキュリティ処理の内容や結果に応じてこれを変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれを変更してもよい。また、ＣＰＵ１２１は、環境設定の内容を示した情報をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からその情報をリードして使用することもできる。この情報は、図２１においてＩＣカード環境設定情報２１１２として示されている。これにより、ＭＭＣ１１０が非活性化されてもその情報を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

【００７４】第１次ＩＣカード初期化処理および第２次ＩＣカード初期化処理は、ＩＣカード制御パラメータＡ、Ｂ、Ｃに設定された値に基づいておこなわれる。また、ＣＰＵ１２１は、ステップ７１２で実行するセキュリティ処理において、ＩＣカード制御パラメータＤに設定された値に基づいてＩＣカードチップ１５０の活性化や非活性化を制御する。

【００７５】図８は、ＩＣカード制御パラメータの種類と設定値、それに対応した処理の内容を表している。まず、パラメータＡは、ＭＭＣ１１０に電源が供給されたときに実行される第１次ＩＣカード初期化処理に関するパラメータである。Ａ＝０のときは、ＣＰＵ１２１はＩＣカードチップ１５０にアクセスしない。Ａ＝１のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットする。Ａ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットした後でＩＣカードチップ１５０の環境設定をおこなう。Ａ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットした後でＩＣカードチップ１５０の環境設定をおこない、最後にＩＣカードチップ１５０を非活性化する。Ａ＝０またはＡ＝３のときは、第１次ＩＣカード初期化処理のあとＩＣカードチップ１５０が非活性状態となる。Ａ＝１またはＡ＝２のときは、第１次ＩＣカード初期化処理のあとＩＣカードチップ１５０は活性状態となる。

【００７６】次に、パラメータＢとＣは、ＭＭＣ１１０がＭＭＣ初期化コマンドを処理したときに実行される第２次ＩＣカード初期化処理に関するパラメータである。Ｂ＝０のときは、ＣＰＵ１２１はＩＣカードチップ１５０にアクセスしない。Ｂ＝１かつＣ＝１のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセット（コールドリセットまたはウォームリセット）する。Ｂ＝１かつＣ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセットした後でＩＣカードチップ１５０の環境設定をおこなう。Ｂ＝１かつＣ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセットした後でＩＣカードチップ１５０の環境設定をおこない、最後にＩＣカ

ードチップ１５０を非活性化する。Ｂ＝２かつＣ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０の環境設定をおこなう。Ｂ＝２かつＣ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０の環境設定をおこなった後にＩＣカードチップ１５０を非活性化する。Ｂ＝３のときは、ＩＣカードチップ１５０が活性状態ならば、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化する。

【００７７】最後に、パラメータＤは、ホスト機器２２０から要求されたセキュリティ処理を実行したあとに、ＩＣカードチップ１５０を非活性化するか否かを示すパラメータである。Ｄ＝０のときは、セキュリティ処理の実行後に、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化せず、活性状態に保つ。Ｄ＝１のときは、セキュリティ処理の実行後に、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化する。

【００７８】ＣＰＵ１２１は、ＩＣカード制御パラメータＡ、Ｂ、Ｃ、Ｄの設定値を変更することができる。ＣＰＵ１２１は、セキュリティ処理の内容や結果に応じてこれらの設定値を変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれらの設定値を変更してもよい。また、ＣＰＵ１２１は、これらの設定値をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からこれらの設定値をリードして使用することもできる。これらの設定値は、図２１においてＩＣカード制御パラメータ２１１１として示されている。これにより、ＭＭＣ１１０が非活性化されてもこれらの設定値を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

【００７９】図９は、第１次ＩＣカード初期化処理の手順を示すフローチャートである。初期化処理を開始する（９０１）と、まず、ＩＣカード制御パラメータＡが０かチェックする（９０２）。Ａ＝０ならばそのまま初期化処理は終了する（９０８）。Ａ＝０でないならばＩＣカードチップ１５０をコールドリセットする（９０３）。次に、ＩＣカード制御パラメータＡが１かチェックする（９０４）。Ａ＝１ならば初期化処理は終了する（９０８）。Ａ＝１でないならばＩＣカードチップ１５０の環境設定をおこなう（９０５）。次に、ＩＣカード制御パラメータＡが２かチェックする（９０６）。Ａ＝２ならば初期化処理は終了する（９０８）。Ａ＝２でないならばＩＣカードチップ１５０を非活性化する（９０７）。そして、初期化処理は終了する（９０８）。

【００８０】図１０は、第２次ＩＣカード初期化処理の手順を示すフローチャートである。初期化処理を開始する（１００１）と、まず、ＩＣカード制御パラメータＢが０かチェックする（１００２）。Ｂ＝０ならばそのまま初期化処理は終了する（１０１３）。Ｂ＝０でないならばＢ＝１かチェックする（１００３）。Ｂ＝１ならばＩＣカード制御パラメータＡが０または３かチェックする（１００４）。Ａが０または３ならば、ＩＣカードチップ１５０をコールドリセットし（１００５）、ステップ１００７に移る。Ａが１または２ならば、ＩＣカードチップ１５０をウォームリセットし（１００６）、ステップ１００７に移る。ステップ１００７では、ＩＣカード制御パラメータＣが１かチェックする。Ｃ＝１ならば初期化処理は終了する（１０１３）。Ｃ＝１でないならばステップ１００９に移る。ステップ１００３においてＢ＝１でないならば、Ｂが２かチェックする（１００８）。Ｂ＝２ならばステップ１００９に移る。Ｂ＝２でないならば、ＩＣカード制御パラメータＡが０または３かチェックする（１０１１）。Ａが０または３ならば初期化処理を終了する（１０１３）。Ａが１または２ならば、ステップ１０１２に移る。ステップ１００９ではＩＣカードチップ１５０の環境設定をおこなう。そして、ＩＣカード制御パラメータＣが２かチェックする（１０１０）。Ｃ＝２ならば初期化処理を終了する（１０１３）。Ｃ＝２でないならばステップ１０１２に移る。ステップ１０１２ではＩＣカードチップ１５０を非活性化する。そして、初期化処理を終了する（１０１３）。

【００８１】図１１は、ＩＣカードチップ１５０が非活性状態であるときに第１次ＩＣカード初期化処理あるいは第２次ＩＣカード初期化処理を実行した場合において、ＩＣカードチップ１５０の外部端子の信号波形を簡単に表した図である。図１２は、ＩＣカードチップ１５０が活性状態であるときに第２次ＩＣカード初期化処理を実行した場合において、ＩＣカードチップ１５０の外部端子の信号波形を簡単に表した図である。図１１と図１２において、時間の方向は左から右にとっており、上の行から下の行に向かってＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。

【００８２】図１１において１１０２は、図３に示したコールドリセットの信号波形を表す。図１２において１２０２は、図４に示したウォームリセットの信号波形を表す。図１１と図１２において、第１設定コマンド処理１１０４ａと１２０４ａ、第２設定コマンド処理１１０４ｂと１２０４ｂ、第Ｎ設定コマンド処理１１０４ｃと１２０４ｃは、それぞれ図５に示したＩＣカードコマンド処理の信号波形を表す。ＩＣカードチップ１５０の環境設定の信号波形１１０４と１２０４は、Ｎ個の設定コマンド処理の信号波形が連なって構成される。

【００８３】図１１と図１２において、１１０６と１２０６は、それぞれ図６に示した非活性化の信号波形を表す。図１１と図１２において、縦方向の破線１１０１、１１０３、１１０５、１１０７、１２０１、１２０３、１２０５、及び１２０７は、それぞれ特定の時刻を表す。１１０１はコールドリセット前の時刻、１２０１はウォームリセット前の時刻、１１０３はコールドリセッ

ト後から環境設定前の間にある時刻、１２０３はウォームリセット後から環境設定前の間にある時刻、１１０５と１２０５は環境設定後から非活性化前の間にある時刻、１１０７と１２０７は非活性化後の時刻である。

【００８４】図１１を参照して、第１次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＡが０のときは、信号波形に変化はない。Ａ＝１のときは、時刻１１０１から時刻１１０３までの範囲の信号波形となる。Ａ＝２のときは、時刻１１０１から時刻１１０５までの範囲の信号波形となる。Ａ＝３のときは、時刻１１０１から時刻１１０７までの範囲の信号波形となる。

【００８５】図１１を参照して、ＩＣカード制御パラメータＡが０または３のときの、第２次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＢが０のときは、信号波形に変化はない。Ｂ＝１かつＩＣカード制御パラメータＣ＝１のときは、時刻１１０１から時刻１１０３までの範囲の信号波形となる。Ｂ＝１かつＣ＝２のときは、時刻１１０１から時刻１１０５までの範囲の信号波形となる。Ｂ＝１かつＣ＝３のときは、時刻１１０１から時刻１１０７までの範囲の信号波形となる。

【００８６】図１２を参照して、ＩＣカード制御パラメータＡが１または２のときの、第２次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＢが０のときは、信号波形に変化はない。Ｂ＝１かつＩＣカード制御パラメータＣ＝１のときは、時刻１２０１から時刻１２０３までの範囲の信号波形となる。Ｂ＝１かつＣ＝２のときは、時刻１２０１から時刻１２０５までの範囲の信号波形となる。Ｂ＝１かつＣ＝３のときは、時刻１２０１から時刻１２０７までの範囲の信号波形となる。Ｂ＝２かつＣ＝２のときは、時刻１２０３から時刻１２０５までの範囲の信号波形となる。Ｂ＝２かつＣ＝３のときは、時刻１２０３から時刻１２０７までの範囲の信号波形となる。Ｂ＝３のときは、時刻１２０５から時刻１２０７までの範囲の信号波形となる。

【００８７】図１３は、図７のステップ７１２において、ＣＰＵ１２１が、ホスト機器２２０が要求したセキュリティ処理をＩＣカードチップ１５０によって実行するときの手順を示すフローチャートである。セキュリティ処理を開始する（１３０１）と、まずＩＣカードチップ１５０が非活性状態かをチェックする（１３０２）。非活性状態ならば、ＩＣカードチップ１５０をコールドリセットし（１３０３）、ステップ１３０６に移る。活性状態ならば、ステップ１３０４に移る。ステップ１３０４では、ＩＣカードチップ１５０にＩＣカードコマンドを発行する前にＩＣカードチップ１５０を再リセットする必要があるかをチェックする。必要があるならば、ＩＣカードチップ１５０をウォームリセットし（１３０５）、ステップ１３０６に移る。必要がないならば、ステップ１３０６に移る。ステップ１３０６では、ＩＣカードチップ１５０の環境設定をおこなう必要があるかをチェックする。必要があるならば、ＩＣカードチップ１５０の環境設定をおこない（１３０７）、ステップ１３０８に移る。必要がないならば、ステップ１３０８に移る。ステップ１３０８では、ＩＣカードチップ１５０のＣＬＫ２端子に供給するクロック信号の周波数Ｆ２を設定する。そして、ＣＰＵ１２１はＩＣカードチップ１５０にセキュリティコマンドを発行し、ＩＣカードチップ１５０はそれを処理する（１３０９）。セキュリティコマンドの処理時間は、クロック周波数Ｆ２に依存する。

【００８８】次に、ＩＣカードチップ１５０が出力するＩＣカードレスポンスにより、その処理が成功したかどうかを判定する（１３１０）。成功ならば、ステップ１３１１に移る。失敗ならば、ステップ１３１２に移る。ステップ１３１１では、ＩＣカードチップ１５０に発行すべきセキュリティコマンドが全て完了したかをチェックする。発行すべきセキュリティコマンドがまだあるならば、ステップ１３０４に移る。発行すべきセキュリティコマンドが全て完了したならば、ステップ１３１４に移る。ステップ１３１２では、失敗したセキュリティコマンドをリトライすることが可能かを判定する。リトライできるなら、リトライ設定をおこない（１３１３）、ステップ１３０４に移る。リトライ設定とは、リトライすべきセキュリティコマンドやその関連データをＣＰＵ１２１が再度準備することである。リトライできないならステップ１３１４に移る。これは、ホスト機器２２０が要求したセキュリティ処理が失敗したことを意味する。ステップ１３１４では、ＩＣカード制御パラメータＤをチェックする。Ｄ＝１ならば、ＩＣカードチップ１５０を非活性化して（１３１５）、セキュリティ処理を終了する（１３１６）。Ｄ＝１でないならば、ＩＣカードチップ１５０を活性状態に保ったままセキュリティ処理を終了する（１３１６）。

【００８９】図１３のフローチャートにおいては、クロック周波数Ｆ２を、ステップ１３０９で発行するセキュリティコマンドの種類によって変えることができるように、ステップ１３０８をステップ１３０９の直前に位置させたが、ステップ１３０８はそれ以外の位置にあってもよい。

【００９０】従来のＩＣカードへの攻撃法を有効にしている要因のひとつとして、ＩＣカードの駆動クロックが外部の接続装置から直接供給されることがあげられる。駆動クロックが接続装置の制御下にあるため、タイミング解析や電力差分解析においては、電気信号の測定においてＩＣカード内部処理のタイミングの獲得が容易になる。一方、故障利用解析においては、異常な駆動クロックの供給による演算エラーの発生が容易になる。これに対し、本発明によれば、ＭＭＣ１１０内部でＩＣカードチップ１５０によりセキュリティ処理を実行するとき、

25

ホスト機器２２０はＩＣカードチップ１５０の駆動クロックを直接供給できない。ＣＰＵ１２１は、ＩＣカードチップ１５０へ供給するクロックの周波数Ｆ２を自由に設定することができる。これにより、ホスト機器２２０の要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。ホスト機器２２０が高速なセキュリティ処理を要求するならば周波数Ｆ２を高く設定し、低い消費電力を要求するならば周波数Ｆ２を低く設定したり、クロックを適度に停止させればよい。

【００９１】また、ＣＰＵ１２１は、周波数Ｆ２だけでなくクロックの供給開始タイミング、供給停止タイミングを自由に設定できる。これらをランダムに変化させることにより、ＩＣカードチップ１５０に対するタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法を困難にすることができる。タイミング解析は、攻撃者が暗号処理１回の処理時間を正確に計測可能であることを仮定しているため、その対策としては、攻撃者が処理時間計測を正確に行えないようにすることが有効である。本発明によりタイミング解析が困難になる理由は、ＩＣカードチップ１５０がＩＣカードコマンドを処理している時間の長さをホスト機器２２０が正確に計測できないためである。電力差分解析の対策としては、処理の実行タイミングや順序に関する情報を外部から検出不可能にすることが有効である。本発明により電力差分解析が困難になる理由は、ＩＣカードコマンドが発行された時刻、発行されたＩＣカードコマンドの内容、発行されたＩＣカードコマンドの順序（ＩＣカードコマンドを複数組み合わせてセキュリティ処理を実行する場合）の検出がホスト機器２２０にとって困難になるためである。故障利用解析の対策としては、ＩＣカードにクロックや電圧や温度等の動作環境検知回路を搭載し、異常を検出したならば処理を停止あるいは使用不能にするという方法が有効である。本発明により故障利用解析が困難になる理由は、ＣＬＫ２制御回路１２７がＩＣカードチップ１５０に異常な駆動クロックを供給しないことが、ホスト機器２２０がＩＣカードチップ１５０に演算エラーを発生させるのを防止するからである。

【００９２】ＣＰＵ１２１は、ＩＣカードチップ１５０に供給するクロックの周波数Ｆ２、供給開始タイミング、及び供給停止タイミングの設定値を、セキュリティ処理の内容や結果に応じて変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機として変更してもよい。また、ＣＰＵ１２１は、これらの設定値をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からこれらの設定値をリードして使用することもできる。これらの設定値は、図２１においてＣＬＫ２設定情報２１１３として示されている。これにより、ＭＭＣ１１０が非活性化されてもこれらの設定値を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

26

【００９３】図１４は、ホスト機器２２０がセキュリティ処理要求ライトコマンドをＭＭＣ１１０に発行してから、ＩＣカードチップ１５０でセキュリティ処理が実行されるまでの過程（図７のステップ７１０～７１２）において、ＭＭＣ１１０およびＩＣカードチップ１５０の外部端子の信号波形、ＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセスを簡単に表した図である。図１４において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、及びＩ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。

【００９４】図１４を参照して、ホスト機器２２０がセキュリティ処理要求ライトコマンドをＭＭＣ１１０に発行してから、ＩＣカードチップ１５０でセキュリティ処理が実行されるまでの過程を説明する。まず、ホスト機器２２０はＣＭＤ端子１４２にセキュリティ処理要求ライトコマンドを送信する（１４０１）。次に、ホスト機器２２０はＣＭＤ端子１４２からセキュリティ処理要求ライトコマンドのレスポンスを受信する（１４０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものであり、セキュリティ処理の実行結果ではない。次に、ホスト機器２２０はＤＡＴ端子１４７にセキュリティ処理要求を送信する（１４０３）。セキュリティ処理要求とは、セキュリティ処理の内容や処理すべきデータを含むホストデータである。次に、ＭＭＣ１１０はＤＡＴ端子１４７をＬレベルにセットする（１４０４）。ＭＭＣ１１０は、これによりビジー状態であることをホスト機器２２０に示す。次に、ＣＰＵ１２１は、ホスト機器２２０から受信したセキュリティ処理要求をフラッシュメモリチップ１３０にライトするコマンドを発行する（１４０５）。セキュリティ処理要求をフラッシュメモリチップ１３０にライトすることにより、ＣＰＵ１２１がセキュリティ処理要求をＩＣカードコマンド形式で記述する処理（図７のステップ７１１）において、ＣＰＵ１２１内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求のデータサイズが大きいときに有効である。

【００９５】なお、フラッシュメモリチップ１３０にライトされたセキュリティ処理要求は、図２１においてセキュリティ処理バッファ領域２１１４に格納される。また、ライトコマンド発行１４０５は必須な操作ではない。ライト処理期間１４０６は、フラッシュメモリチップ１３０がセキュリティ処理要求のライト処理を実行している期間を表す。セキュリティ処理１４０７はＩＣカードチップ１５０によるセキュリティ処理の信号波形を

表す。この信号波形は図１３のフローチャートの遷移過程に依存する。セキュリティ処理１４０７は、ライト処理期間１４０６とオーバラップさせることができる。一般にフラッシュメモリチップ１３０のライト処理期間１４０６はミリ秒のオーダーであるため、セキュリティ処理１４０７とオーバラップさせることは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。リード／ライト１４０８は、セキュリティ処理１４０７の実行中に、フラッシュメモリチップ１３０からセキュリティ処理要求をリードしたり、ＩＣカードチップ１５０が出力した計算結果をフラッシュメモリチップ１３０にライトするアクセスを示している。このアクセスにより、ＣＰＵ１２１内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求やセキュリティ処理結果のデータサイズが大きいときに有効である。リード／ライト１４０８は必須ではない。セキュリティ処理１４０７が完了したら、ＭＭＣ１１０はＤＡＴ端子１４７をＨレベルにセットする（１４０９）。ＭＭＣ１１０は、これによりセキュリティ処理が完了したことをホスト機器２２０に示す。

【００９６】図１５は、図１４におけるセキュリティ処理１４０７の信号波形の一例を表した図である。図１５において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、及びＩ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。１５０１は図３に示したコールドリセットの信号波形を表し、１５０４は図４に示したウォームリセットの信号波形を表し、１５０２および１５０５は図１１（あるいは図１２）に示した環境設定の信号波形を表し、１５０３および１５０６および１５０７は図５に示したＩＣカードコマンド処理の信号波形を表し、１５０８は図６に示した非活性化の信号波形を表す。ＩＣカードチップ１５０の外部端子において図１５に示した信号波形が観測されるのは、図１３のフローチャートが１３０１、１３０２、１３０３、１３０６、１３０７、１３０８、１３０９、１３１０、１３１１、１３０４、１３０５、１３０６、１３０７、１３０８、１３０９、１３１０、１３１１、１３０４、１３０６、１３０８、１３０９、１３１０、１３１１、１３１４、１３１５、１３１６の順で遷移するときである。

【００９７】図１５を参照して、図１４のセキュリティ処理１４０７の実行中におけるＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセス（リード／ライト１４０８）を説明する。このアクセスには、図２１におけるセキュリティ処理バッファ領域２１１４を使用する。リード１５０９、１５１１、及び１５１２は、それぞれ、セキュリティコマンド処理１５０３、１５０６、及び１５０７においてＩＣカードチップ１５０に送信するＩＣカードコマンドを構築するために必要なデータを、フラッシュメモリチップ１３０からリードするアクセスである。ライト１５１０は、セキュリティコマンド処理１５０３においてＩＣカードチップ１５０が出力した計算結果を、フラッシュメモリチップ１３０にライトするアクセスである。ライト１５１３は、セキュリティコマンド処理１５０６及び１５０７においてＩＣカードチップ１５０が出力した計算結果を、フラッシュメモリチップ１３０にまとめてライトするアクセスである。リード１５０９、１５１１、１５１２は、それぞれ、セキュリティコマンド処理１５０３、１５０６、１５０７以前のＩＣカードチップ１５０へのアクセスとオーバラップさせることができる。ライト１５１０、１５１３は、それぞれ、セキュリティコマンド処理１５０３、１５０７以後のＩＣカードチップ１５０へのアクセスとオーバラップさせることができる。これらのオーバラップは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。さらに、フラッシュメモリチップ１３０のライト単位が大きい場合は、ライト１５１３のように複数の計算結果をまとめてライトすることができる。これは、フラッシュメモリチップ１３０へのライト回数を削減し、フラッシュメモリチップ１３０の劣化を遅らせる効果がある。なお、ライト１５１０、１５１３でフラッシュメモリチップ１３０にライトする内容は、ＩＣカードチップ１５０が出力した計算結果そのものに限定されず、図７のステップ７１５でホスト機器２２０に返すセキュリティ処理結果またはその一部であってもよい。この場合、図７のステップ７１４またはその一部は、ステップ７１２の中で実行されることになる。

【００９８】図１６は、ホスト機器２２０がセキュリティ処理結果リードコマンドをＭＭＣ１１０に発行してから、ＭＭＣ１１０がセキュリティ処理結果を出力するまでの過程（図７のステップ７１３～７１５）において、ＭＭＣ１１０の外部端子の信号波形、ＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセスを簡単に表した図である。図１６において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、及びＤＡＴ端子１４７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。

【００９９】図１６を参照して、ホスト機器２２０がセキュリティ処理結果リードコマンドをＭＭＣ１１０に発行してから、ＭＭＣ１１０がセキュリティ処理結果を出力するまでの過程を説明する。まず、ホスト機器２２０はＣＭＤ端子１４２にセキュリティ処理結果リードコマンドを送信する（１６０１）。次に、ホスト機器２２０はＣＭＤ端子１４２からセキュリティ処理結果リードコ

マンドのレスポンスを受信する（１６０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものであり、セキュリティ処理結果ではない。次に、ＭＭＣ１１０はＤＡＴ端子１４７をＬレベルにセットする（１６０３）。ＭＭＣ１１０は、これによりビジー状態であることをホスト機器２２０に示す。次に、ＣＰＵ１２１は、フラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）から、ＩＣカードチップ１５０が出力した計算結果をリードする（１６０４）。ＣＰＵ１２１は、これをもとにセキュリティ処理結果を構築し、ＭＭＣ１１０がＤＡＴ端子１４７にセキュリティ処理結果を出力する（１６０５）。なお、図７のステップ７１４またはその一部が、ステップ７１２の中で実行されている場合、ステップ１６０４ではフラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）からセキュリティ処理結果またはその一部をリードする。なお、フラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）を利用しないでセキュリティ処理結果を構築する場合、ステップ１６０４は必要ない。

【０１００】ＭＭＣ１１０の製造者や管理者は、セキュリティシステムのユーザにＭＭＣ１１０を提供する前やそのユーザが所有するＭＭＣ１１０に問題が発生した時に、ＭＭＣ１１０に内蔵されたＩＣカードチップ１５０に様々な初期データを書きこんだり、ＩＣカードチップ１５０のテストをおこなったりする必要がある。ＭＭＣ１１０の製造者や管理者によるこれらの操作の利便性を高めるために、ＭＭＣ１１０は、ＩＣカードチップ１５０の外部端子をＭＭＣ外部端子１４０に割りつけるインタフェース機能を持つ。これにより、図３～図６で示したようなＩＣカードチップ１５０へのアクセス信号を、ＭＭＣ外部端子１４０から直接送受信できる。このようなＭＭＣ１１０の動作モードを、ＭＭＣ仕様に準拠した動作モードと区別して、以下、インタフェース直通モードと呼ぶ。

【０１０１】インタフェース直通モードについて詳細に説明する。図１７は、ＩＣカードチップ１５０の外部端子をＭＭＣ外部端子１４０に割りつけるときの対応関係の一例を表した図である。この例では、ＲＳＴ端子１５２をＣＳ端子１４１に割り付け、ＧＮＤ２端子１５５をＧＮＤ１端子１４３、１４６に割り付け、ＶＣＣ２端子１５１をＶＣＣ１端子１４４に割り付け、ＣＬＫ２端子１５３をＣＬＫ１端子１４５に割り付け、Ｉ／Ｏ端子１５７をＤＡＴ端子１４７に割り付ける。このとき、ＣＳ端子１４１とＣＬＫ１端子１４５は入力端子、ＤＡＴ端子１４７は入出力端子として機能する。

【０１０２】ＭＭＣ１１０は、特定のメモリカードコマンドを受信すると、動作モードをインタフェース直通モードへ移したり、インタフェース直通モードからＭＭＣ仕様に準拠した動作モードに戻すことができる。以下、動作モードをインタフェース直通モードへ移すメモリカードコマンドを直通化コマンド、動作モードをインタフェース直通モードから通常の状態に戻すメモリカードコマンドを復帰コマンドと呼ぶ。図１を参照して、ＭＭＣＩ／Ｆ制御回路１２３は、ＶＣＣ２制御回路１２６、ＣＬＫ２制御回路１２７、ＩＣカードＩ／Ｆ制御回路１２８と接続されており、ＭＭＣ１１０がホスト機器２２０から直通化コマンドを受信すると、ＣＰＵ１２１の指示により図１７で示した端子割り付けをおこなう。ＭＭＣ１１０がホスト機器２２０から復帰コマンドを受信すると、ＣＰＵ１２１の指示により図１７で示した端子割り付けを解除し、ＭＭＣ１１０はＭＭＣ仕様に準拠した動作モードに戻る。

【０１０３】インタフェース直通モードでは、ホスト機器２２０がＩＣカードチップ１５０に直接アクセスできるため、セキュリティの観点からインタフェース直通モードを利用できるのは限られた者だけにする必要がある。そこで、直通化コマンドの発行には、一般のユーザに知られないパスワードの送信を必要とする。正しいパスワードが入力されないとインタフェース直通モードは利用できない。

【０１０４】図１８は、ホスト機器２２０が、ＭＭＣ１１０の動作モードをＭＭＣ仕様に準拠した動作モードからインタフェース直通モードに移し、ＩＣカードチップ１５０に直接アクセスし、その後、ＭＭＣ１１０の動作モードを再びＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードに戻すまでの処理手順を示すフローチャートである。ホスト機器２２０は処理を開始し（１８０１）、まずＭＭＣ１１０に直通化コマンドを発行する（１８０２）。ＭＭＣ１１０は、直通化コマンドで送信されたパスワードが正しいかチェックする（１８０３）。正しければステップ１８０４に移り、間違っていれば処理は終了する（１８１０）。ステップ１８０４では、ＣＰＵ１２１は、ＩＣカードチップ１５０をコールドリセットする。そして、図１７で示した端子割り付けをおこないインタフェースを直通化する（１８０５）。この時点から、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスする（１８０６）。ホスト機器２２０がＩＣカードチップ１５０への直接アクセスを終了し、ＭＭＣ１１０の動作モードを再びＭＭＣ仕様に準拠した動作モードに戻すときは、ＭＭＣ１１０に復帰コマンドを発行する（１８０７）。すると、ＣＰＵ１２１は図１７で示した端子割り付けを解除し、ＭＭＣ１１０はＭＭＣ仕様に準拠した動作モードに戻る（１８０８）。そして、ＣＰＵ１２１は、ＩＣカードチップ１５０を非活性化する（１８０９）。以上で、処理は終了する（１８１０）。

【０１０５】図１９は、図１８のステップ１８０１～１８０６の過程において、ＭＭＣ１１０およびＩＣカード

チップ１５０の外部端子の信号波形を簡単に表した図である。図１９において、時間の方向は左から右にとる。上の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、及びＩ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。１９０５は、図３のコールドリセットの信号波形を示す。モード移行時刻１９０６は、動作モードがインタフェース直通モードに移る時刻を表す。

【０１０６】図１９を参照して、ホスト機器２２０がＭＭＣ１１０の動作モードをＭＭＣ仕様に準拠した動作モードからインタフェース直通モードに移しＩＣカードチップ１５０に直接アクセスする過程を説明する。なお、ＭＭＣ１１０のＶＣＣ１端子１４４には３Ｖ（ＶＣＣ２端子１５１の標準電圧）が供給されている。ホスト機器２２０がＣＭＤ端子１４２に直通化コマンドを入力すると（１９０１）、ＣＭＤ端子１４２から直通化コマンドのレスポンスが出力される（１９０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものである。次に、ホスト機器２２０はＤＡＴ端子１４７にパスワードを入力する（１９０３）。パスワード入力後、ＭＭＣ１１０はＤＡＴ端子１４７にＬレベルを出力し（１９０４）、ビジー状態であることをホスト機器２２０に示す。ビジー状態の間に、ＣＰＵ１２１は、ＩＣカードチップ１５０をコールドリセットする（１９０５）。そして、モード移行時刻１９０６において、動作モードをインタフェース直通モードに移す。このときに、ＤＡＴ端子１４７はＬレベルからハイインピーダンス状態になる。これにより、ホスト機器２２０はビジー状態の解除を知ることができる。この時点から、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスする。例えば、ＣＬＫ１端子１４５にクロックを供給すると（１９０７）、ＣＬＫ２端子１５３にそのクロックが供給される（１９０８）。また、ＤＡＴ端子１４７にＩＣカードコマンドを送信すると（１９０９）、Ｉ／Ｏ端子１５７にそのＩＣカードコマンドが送信される（１９１０）。

【０１０７】図２０は、図１８のステップ１８０７～１８１０の過程において、ＭＭＣ１１０およびＩＣカードチップ１５０の外部端子の信号波形を簡単に表した図である。図２０において、時間の方向は左から右にとる。上の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、及びＩ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。モード復帰時刻２００３は、動作モードがインタフェース直通モードからＭＭＣ仕様に準拠した動作モードに戻る時刻を表す。２００４は、図６の非活性化の信号波形を示す。

【０１０８】図２０を参照して、ホスト機器２２０がＭＭＣ１１０の動作モードをインタフェース直通モードからＭＭＣ仕様に準拠した動作モードに戻す過程を説明する。なお、ＭＭＣ１１０のＶＣＣ１端子１４４には３Ｖ（ＶＣＣ２端子１５１の標準電圧）が供給されている。ホスト機器２２０がＣＭＤ端子１４２に復帰コマンドを入力すると（２００１）、ＣＭＤ端子１４２から復帰コマンドのレスポンスが出力される（２００２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものである。そして、モード復帰時刻２００３において、ＭＭＣ１１０はＤＡＴ端子１４７にＬレベルを出力してビジー状態であることをホスト機器２２０に示し、それと同時に動作モードをＭＭＣ仕様に準拠した動作モードに戻す。ビジー状態の間に、ＣＰＵ１２１は、ＩＣカードチップ１５０を非活性化する（２００４）。そして、ＭＭＣ１１０は、ＤＡＴ端子１４７をハイインピーダンス状態にし（２００５）、復帰コマンドの処理が完了したことをホスト機器２２０に示す。これ以後、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスできない。ホスト機器２２０が、ＣＬＫ１端子１４５にクロックを供給しながらＣＭＤ端子１４２に何らかのメモリカードコマンドを送信した場合、ＩＣカードチップ１５０にそのクロック信号（２００６）は伝わらない。２００１及び２００２においてホスト機器２２０がＣＬＫ１端子１４５に供給するクロック信号は、ＩＣカードチップ１５０のＣＬＫ２端子１５３にも伝わるが、ＤＡＴ端子１４７がハイインピーダンス状態であるため、ＩＣカードチップ１５０がＩＣカードコマンドを誤って認識することはない。

【０１０９】図２１において、セキュリティ処理ステータス領域２１１６には、ＩＣカードチップ１５０によるセキュリティ処理の進捗状況を示す情報を格納する。ＣＰＵ１２１は、この情報をセキュリティ処理の実行中に更新することができる。例えば、セキュリティ処理の途中でＭＭＣ１１０への電源供給が停止した場合、電源供給再開時にＣＰＵ１２１がこの情報をリードして参照すれば、セキュリティ処理を中断した段階から再開することができる。

【０１１０】本発明におけるＭＭＣ１１０は、コントローラチップ１２０、フラッシュメモリチップ１３０及びＩＣカードチップ１５０の三つのうち二つ以上のチップで同時に処理を行うことで、処理の高速化及び処理時間の短縮を図ることができる。以下、本発明を適用したＭＭＣ１１０で行える並列処理の動作について説明する。

図２７は、並列に処理できるデータリード処理の手順を示したフローチャートである。ホスト機器２２０とＭＭＣ１１０は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態２７０１、待機状態２７１９となっている。ホスト機器２２０がＭＭＣ

１１０のＣＭＤ端子１４２に第一コマンドを送信すると（２７０２）、ＭＭＣ１１０は、第一コマンドを受信し（２７０９）、第一レスポンスを返す（２７１０）。ここで、レスポンスとは、コマンドを受け取ったＭＭＣ１１０がホスト機器２２０に返すデータのことである。単にコマンドを受信したら返すデータであるので、レスポンスを返すことがコマンドの実行が終了したことを意味しない。

【０１１１】ＭＭＣ１１０のコントローラチップ１２０は、第一コマンドを解釈し、フラッシュメモリチップ１３０又はＩＣカードチップ１５０に制御命令を発し第一処理に入る（２７１５）。ホスト機器２２０は、第一レスポンスを受け取ると第二コマンドを送信する（２７０４）。ＭＭＣ１１０のコントローラチップ１２０は、第一処理を実行しながら、ホスト機器２２０より第二コマンドを受信し、（２７０５）、第二レスポンスを返す（２７１２）。コントローラチップ１２０は、第二コマンドを解釈し、第二処理を実行する（２７１３）。

【０１１２】第二コマンドは、あらかじめ第一コマンドと同時に処理できるコマンドをホスト機器２２０で判定し設定する。また、同時に処理できるコマンドの判定は、コントローラチップ１２０でおこなってもよい。以下、同時に実行できるコマンドのことを並列実行可能なコマンドと呼ぶ。並列実行可能なコマンドとしては、例えば、フラッシュメモリチップ１３０にアクセスするコマンドとＩＣカードチップ１５０にアクセスするコマンド等の異なったチップにアクセスするコマンドである。例えば、フラッシュメモリチップ１３０から音楽データを読み出すコマンドが第一コマンドに相当し、暗号化されたデータを復号化する処理を実行するコマンドが第二コマンドに相当する。

【０１１３】第一処理が終了すると、コントローラチップ１２０は、ホスト機器２２０に第一データを送信する（２７１６）。その後、第二データを送信する（２７１４）。第一データ及び第二データの区別は、ＭＭＣ１１０のコントローラチップ１２０とホスト機器２２０のホストインターフェース２２３でデータに識別情報を付加して管理判断する。以下、識別情報を付加したデータをデータと呼ぶ。

【０１１４】また、第一処理の転送が終了して、第二処理をしている間にホスト機器２２０が並列実行可能なコマンドを第三コマンドとして発行した場合は、コントローラチップ１２０は、第二処理の実行とあわせて第三コマンドのコマンドを解釈し、第三処理を実行する（２７１７）。もし第一コマンドが大容量のデータ（ストリームデータ等）を要求するコマンドであるならば、第三処理を実行し（２７１７）、第二データの送信の終了を待ち、第三データを送信する（２７１８）。その後ホスト機器２２０からコマンドがなければ、ＭＭＣ１１０は待機状態になる（２７１９）。ホスト機器２２０はＭＭＣ１１０から必要なデータを受け取ると、待機状態になる（２７０１）。

【０１１５】図２８は、リードコマンドを並列処理する時のコマンドとデータの流れ、処理を時間軸にそって示した図である。ホスト機器２２０は、ＭＭＣ１１０のＣＭＤ端子１４２に第一コマンドを送信する（２７０２）。コントローラチップ１２０は、第一コマンドを解釈し、フラッシュメモリチップ１３０に制御命令を出す。第一処理中（２７１５）に、ホスト機器２２０は、並列実行可能なコマンドを第二コマンドとしてＭＭＣ１１０のＣＭＤ端子１４２に送信する（２７０４）。コントローラチップ１２０は、第二コマンドを解釈し、ＩＣカードチップ１５０に制御命令を出し、第二処理を実行する（２７１３）。ＭＭＣ１１０は、第一データ２８０３、第二データ２８０４のように順にデータを転送する。第二処理（２７１３）中にホスト機器２２０が第三コマンドとしてフラッシュメモリチップ１３０にアクセスするコマンドを発行した場合（２８０１）、コントローラチップ１２０はフラッシュメモリチップに制御命令を出す。ＭＭＣ１１０は、第二データ２８０４の転送終了を待って、第三データ２８０５を転送する。また第三データ２８０５は、第一コマンドが大容量データ（ストリームデータ等）を送るコマンドでもよい。その場合は、第三コマンドの発行（２８０１）と第三レスポンス（２８０２）の信号はなくてもよい。以上の処理内容は、コントローラチップ１２０が制御命令を出す対象としてフラッシュメモリチップ１３０がＩＣカードチップ１５０で、ＩＣカードチップ１５０がフラッシュメモリチップ１３０のように逆の場合でもよい。

【０１１６】図２９は、並列に処理できるデータライト処理の流れを示した図である。ホスト機器２２０とＭＭＣ１１０は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態２９０１及び待機状態２９１０となっている。ホスト機器２２０がＭＭＣ１１０のＣＭＤ端子１４２に第一コマンドを送信する（２９０２）。ＭＭＣ１１０は、第一コマンドを受信し（２９１１）、第一レスポンスを返し（２９１２）、同時に第一データを受信し（２９１３）、データ端子１４７からデータを転送できないようにする。これを以下ビジー状態と呼ぶ。ＭＭＣ１１０はホスト機器２２０からデータを受け取った後ビジー状態にしなくても良い。第一データを受信するステップ２９１３は、第一レスポンス（２９１２）と同時でなくても良い。

【０１１７】ホスト機器２２０は、第一レスポンスを受信し（２９０３）、並列実行可能なコマンドを第二コマンドとして、ＣＭＤ端子１４２に送信する（２９０４）。ＭＭＣ１１０は、ホスト機器２２０より第二コマンドを受信し（２９１４）、第一データを受信（２９１３）中であれば受信し、第二レスポンスを送信し（２９１５）、第二処理を開始する（２９２０）。データビジ

一状態であれば、第二処理で行うアドレス設定まで行い、第二データの転送を待つ。第二処理はアドレス設定のみだけでなく実行可能な処理を続けてもよい。ホスト機器２２０は、第二レスポンスを受信し（２９０５）、ビジー状態の解除を待って、第二データを送信する（２９０７）。第一コマンドが大容量データ（ストリームデータ等）を転送する場合、ＭＭＣ１１０は、第二処理中（２９２０）に第三処理を開始し（２９２１）、第三データの転送（２９０８）を待つ。ＭＭＣ１１０は、ビジー状態が解除されたら、第三データを受信し（２９１８）、第三処理を続ける。その後ホスト機器２２０からコマンドがなければ、ＭＭＣ１１０は待機状態になる（２９１０）。ホスト機器２２０はＭＭＣ１１０に必要なデータを転送し終わると、待機状態になる（２９０１）。

【０１１８】図３０は、ライトコマンドを並列処理する時のコマンドとデータの流れ及び処理を時間軸にそって示した図である。ホスト機器２２０がフラッシュメモリチップ１３０にデータをライトする第一コマンドをＭＭＣ１１０のＣＭＤ端子１４２に送信し（２９０２）、第一レスポンスを待ち（２９０３）、第一データを送信する（３００３）。ＭＭＣ１１０は、第一コマンドを受けると第一レスポンスを送信し（２９０３）、フラッシュメモリチップ１３０に制御命令を出し（第一処理２９１６）、ビジー状態となる。ここでビジー状態にしなくてもよい。ホスト機器２２０は、第一データ３００３を送信しながら並列実行可能なコマンドとしてＩＣカードチップ１５０にデータを転送する第二コマンドを送信する（２９０４）。ホスト機器２２０は、第二レスポンスを受信し（２９０５）、ビジー状態の解除を待って第二データ３００４を送信する。コントローラチップ１２０は、ＩＣカードチップ１５０に制御命令を出し、第二処理を開始して、第二データ３００４を待つ。ホスト機器２２０は、ビジー状態が解除されるとＩＣカードチップ１５０に送信する第二データ３００４を転送する。

【０１１９】ＭＭＣ１１０は、第二データを受信すると（２９１７）、ビジー状態になる。ＩＣカードチップ１５０が処理中（第二処理中２９２０）に、ホスト機器２２０がフラッシュメモリチップ１２０にアクセスする第三コマンドの発行すると（３００１）、ＭＭＣ１１０は、第三レスポンスを送信し（３００２）、コントローラチップ１２０はフラッシュメモリチップに制御命令を出し、第三処理を開始する（２９２１）。ホスト機器２２０は、ビジー状態の解除を待って第三データを送信する（３００５）。もしフラッシュメモリチップ１３０にアクセスする第一コマンドが大容量データ（ストリームデータ等）を転送する場合は、ICカードチップ１５０の処理中（第二処理２９２０）のビジー状態の解除を待って、ホスト機器２２０は、フラッシュメモリチップ１３０に第三データ３００５を送信する。ＭＭＣ１１０は、第三データ３００５を受信し、フラッシュメモリチップ１３０に制御命令を出し第三処理を行う。

【０１２０】以上の処理内容は、コントローラチップ１２０が制御命令を出す対象としてフラッシュメモリチップ１３０がＩＣカードチップ１５０で、ＩＣカードチップ１５０がフラッシュメモリチップ１３０のように逆の場合でもよい。

【０１２１】図３１は、並列に処理できるデータを転送しないコマンドの処理を示した図である。ホスト機器２２０及びＭＭＣ１１０は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態３１０１、待機状態３１１０となっている。ホスト機器２２０はＭＭＣ１１０のＣＭＤ端子１４２に第一コマンドを送信する（３１０２）。ＭＭＣ１１０は、第一コマンドを受信し（３１１１）、第一レスポンスをホスト機器２２０に送信し（３１１２）、第一処理を開始する（３１１６）。ホスト機器２２０はＭＭＣ１１０からの第一レスポンスを受信すると（３１０３）、並列実行可能なコマンドを第二コマンドとして送信する（３１０４）。ＭＭＣ１１０は、第二コマンドを受信すると（３１１３）、ホスト機器２２０に対し第二レスポンスを送信し（３１１４）、第二処理を実行する（３１１５）。その後処理が終わると、ホスト機器２２０は待ち状態３１０１、ＭＭＣ１１０は待ち状態３１１０の状態となる。

【０１２２】図３２は、並列に処理できるデータを転送しないコマンドの実行する時の処理を時間軸にそって示した図である。ホスト機器２２０は、ＭＭＣ１１０のＣＭＤ端子１４２にデータ転送を行わないフラッシュメモリチップ１３０にアクセスする第一コマンドを送信する（３１０２）。ＭＭＣ１１０は、第一コマンドを受信し（３１１１）、コントローラチップ１２０は、フラッシュメモリチップ１３０に制御命令を出し、第一処理を開始する（３１１４）。ホスト機器２２０は、第一レスポンスを受信し（３１０３）、ＭＭＣ１０のＣＭＤ端子１４２にデータ転送を行わないＩＣカードチップ１５０にアクセスする第二コマンドを送信する（３１０４）。ＭＭＣ１１０は、第二コマンドを受信し（３１１３）、コントローラチップ１２０は、ＩＣカードチップ１５０に制御命令を出し第二処理を行う（３１１５）。ホスト機器２２０は、コントローラチップ１２０の内部処理のみで実行できるコマンドを第三コマンドとしてＭＭＣ１１０のＣＭＤ端子１４２に送信する（３２０１）。ＭＭＣ１１０は第三コマンドを受信し、第三処理を実行する（３２０３）。このとき、第一処理及び第二処理は実行中でもよい。

【０１２３】以上の処理の中で、第一コマンド及び第二コマンドは、フラッシュメモリチップ１３０にアクセスする処理、ＩＣカードチップ１５０にアクセスする処理、及びコントローラチップ１２０の内部処理の三処理のうちのどの二処理でもよい。また、連続コマンドが、

コントローラチップ１２０の内部処理のみで実行できるコマンドで、同様の処理を行うコマンドは、後で発行したコマンドだけを有効にしても良い。

【０１２４】図３３は、並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを示した図である。ホスト機器２２０及びMMC１１０は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態３３０１、待機状態３３１０となっている。ホスト機器２２０がMMC１１０のCMD端子１４２に第一コマンドを送信する（３３０２）。MMC１１０は第一コマンドを受信し（３３１１）、第一レスポンスをホスト機器２２０に送信し（３３１２）、第一処理を開始する（３３１６）。ホスト機器２２０は、第一レスポンスを受信して（３３０３）、並列実行可能なコマンドを第二コマンドとして送信する（３３０４）。MMC１１０は、第二コマンドを受信し（３３１３）、第二レスポンスを返す（３３１４）。その間にDAT端子１４７から、第一データを送信し（３３１７）、第二処理を開始する（３３１５）。ホスト機器２２０は、第一データを受信し（３３０６）、第二レスポンスを受信する（３３０５）。ホスト機器２２０は、並列処理可能なコマンドとして第三コマンドを送信する（３３０７）。MMC１１０は、第三コマンドを受信し（３３１８）、第三レスポンスを返す（３３１９）。ホスト機器２２０は、第三レスポンス受信する（３３０８）。MMC１１０は、第三処理３１２０を実行し、第二データを送信する（３３２１）。ホスト機器２２０は、第二データを受信する（３３０９）。その後実行するコマンドがなければ、ホスト機器２２０は、待ち状態３３０１に、MMC１１０は、待ち状態３３１０になる。

【０１２５】図３４は、並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。ホスト機器２２０がMMC１１０のコマンド端子１４２にフラッシュメモリチップ１２０にアクセスする第一コマンドを送信する（３３０２）。MMC１１０は第一レスポンスを返し（３３０３）、コントローラチップ１２０は、制御命令をフラッシュメモリチップ１３０に出し第一処理を開始する（３３１７）。ホスト機器２２０は、並列実行可能なデータ転送を伴わないＩＣカードチップ１５０にアクセスする第二コマンドを送信する（３３０４）。MMC１１０は第二コマンドを受信して（３３１３）、第二レスポンスを返し（３３０５）、コントローラチップ１２０はＩＣカードチップ１５０に制御命令を出し、第二処理を開始する（３３１５）。MMC１１０は、第一処理が終了すると（３３１６）、第一データ３４０３をホスト機器２２０に送信する。ホスト機器２２０は、第一データを受信し（３３０６）、並列処理可能なフラッシュメモリチップ１３０にアクセスする第三コマンドを送信する（３３０７）。MMC１１０は、第三レスポンスを返し（３３０８）、コントローラチップ１２０は第三処理を実行し（３３２０）、第二データを送信する（３４０５）。

【０１２６】以上の処理は、フラッシュメモリトップ１３０がＩＣカードチップ１５０で、ＩＣカードチップ１５０がフラッシュメモリチップ１３０のように逆でもよい。また、データ転送を伴わないコマンドは、コントローラチップ１２０の内部処理を行うコマンドでもよい。第一コマンドが大容量データデータ（ストリームデータなど）を転送するコマンドの場合は、第三コマンドは、発行されなくても良い。

【０１２７】図３５は、並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを示した図である。ホスト機器２２０及びMMC１１０は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態３５０１、待機状態３５１０となっている。ホスト機器２２０がMMC１１０のCMD端子１４２に第一コマンドを送信する（３５０２）。MMC１１０は第一コマンドを受信し（３５１１）、第一レスポンスをホスト機器２２０に送信する（３５１２）。ホスト機器２２０は、第一レスポンスを受信して（３５０３）、並列実行可能なコマンドを第二コマンドとして送信し（３５０４）、第一データを送信する（３５０５）。MMC１１０は、第二コマンドを受信し（３５１３）、第二レスポンスを返す（３５１４）。その間にDAT端子１４７から、第一データを受信し（３５１６）ビジー状態になる。MMC１１０は、第一データを受信したら（３５１６）、第一処理を開始し（３５１７）、第二処理を開始する（３５１５）。ホスト機器２２０は、ビジー状態が解除されると第三コマンドを送信（３５０７）する。MMC１１０は第三レスポンスを返す（３５１９）。ホスト機器１１０は第三レスポンスを受信すると（３５０８）、第二データを送信する（３５０９）。MMC１１０は、第二データを受信し（３５２０）、ビジー状態になり第三処理（３５２１）を実行する。処理が終了すると、ホスト機器２２０は、待ち状態３５０１となり、MMC１１０は処理が終了すると待ち状態３５１０となる。以上の処理で、MMC１１０がデータ受信後ビジー状態にならなくても良い。

【０１２８】図３６は、並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。ホスト機器２２０がフラッシュメモリチップ１３０にアクセスする第一コマンドを転送する（３５０２）。MMC１１０は第一レスポンスを返し（３５０３）、第一データ受信し（３５０５）、コントローラチップ１２０はフラッシュメモリチップ１３０に制御命令を出し、第一処理を開始し（３５１７）、ビジー状態となる。ホスト機器２２０は、並列実行可能なデータ転送を伴わないＩＣカードチップ１５０にアクセスする第二コマンドを送信する（３５０４）。MMC１１０は第二コマンドを受信して（３５１

３）、第二レスポンスを返す（３５０６）。コントローラチップ１２０は、ＩＣカードチップ１５０に制御命令をだし第二処理を開始する（３５１５）。その後ホスト機器２２０はビジー状態が解除されるのを待って、フラッシュメモリチップ１３０にアクセスする第三コマンドを送信する（３５０７）。ＭＭＣ１１０は、第三コマンドを受信し（３５１８）、第三レスポンスを返し（３５０８）、第二データ３５０９を受信する（３５２０）。コントローラチップ１２０は、フラッシュメモリチップ１３０に制御命令を出し、第三処理を開始しビジー状態になる（３５２１）。

【０１２９】以上の処理で、フラッシュメモリチップ１３０がＩＣカードチップ１５０に、ＩＣカードチップ１５０がフラッシュメモリチップ１３０のように逆になっても良い。データ転送を伴わない処理は、コントローラチップ１２０の内部処理でもよい。また、ＭＭＣ１１０がデータ受信後ビジー状態にならなくても良い。第一コマンドが大容量データ（ストリームデータ等）を転送するコマンドである場合、第三コマンドの発行と第三レスポンスは必要としない。

【０１３０】以上の動作は、図２４及び図２５で示す、ＳＤカードホスト機器２４６０とSDカード２４１０、メモリスティックホスト機器２５６０とメモリスティック２５１０のような構成で、コントローラを通してのＳＤカード内のＩＣカードチップ１５０とフラッシュメモリチップ２４３０、メモリスティック内のＩＣカードチップ１５０とフラッシュメモリチップ２５３０の同時アクセスの場合においても同様である。

【０１３１】以上のように、ホストからのコマンドに応じて、フラッシュメモリチップ１３０、ＩＣカードチップ１５０及びコントローラチップ１２０で並列処理が可能であるので処理を高速化及び処理時間を短縮することができる。したがって、一つのＭＭＣ１１０を用いて、音楽データを再生しながら、銀行からお金を引き落とす際の認証処理を行うことができる。

【０１３２】本発明の実施形態によれば、メモリカード外部からＩＣチップの駆動クロックを直接供給しないため、ＩＣチップの処理時間を正確に計測できず、また、処理の実行タイミングや順序の検出が困難になる。さらに、異常な駆動クロックを供給することができず、演算エラーを発生させるのが困難になる。したがって、タイミング解析、電力差分解析、故障利用解析攻撃法に対するセキュリティが向上する。

【０１３３】本発明の実施形態によれば、メモリカード外部からＩＣチップの制御方式を自由に設定できる。例えば、高速処理が要求されるならば、ＩＣチップの駆動クロックの周波数を高くした制御方式を設定し、低消費電力が要求されるならば、ＩＣチップの駆動クロックの周波数を低くしたり、ＩＣチップの駆動クロックを適度に停止させる制御方式を設定することができる。したがって、セキュリティシステムの要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。

【０１３４】本発明の実施形態によれば、ＩＣチップによるセキュリティ処理に必要なデータや、ＩＣチップを管理するための情報を、フラッシュメモリに保持することができる。したがって、セキュリティ処理の利便性を向上させることができる。

【０１３５】本発明の実施形態によれば、ＭＭＣの製造者や管理者が、ＭＭＣ内部のＩＣチップに直接アクセスすることができる。したがって、ＭＭＣ内部のＩＣチップの初期化やメンテナンスを、従来のＩＣカードと同様な方法で実現できる。

【０１３６】本発明の実施形態によれば、フラッシュメモリチップを備えたＭＭＣに、セキュリティ機能を追加する場合、セキュリティ評価機関の認証を予め受けたＩＣカードチップ追加搭載することによって、セキュリティ評価機関によるＭＭＣの認証が不要となるため、ＭＭＣの開発期間又は製造期間が短縮する。

【０１３７】本発明の実施形態によれば、ホスト機器からのコマンドに応じて、フラッシュメモリチップ、ＩＣカードチップ及びコントローラチップ１２０で並列処理が可能であるので処理を高速化することができる。

【０１３８】

【発明の効果】本発明によれば、記憶装置のセキュリティを向上するという効果を奏する。また、記憶装置の処理を高速にすることができる。

【図面の簡単な説明】

【図１】本発明を適用したＭＭＣ１１０の内部構成を示す図である。

【図２】本発明を適用したＭＭＣ１１０のホスト機器２２０の内部構成、およびホスト機器とＭＭＣ１１０との接続状態を示す図である。

【図３】ＩＣカードチップのコールドリセット時の信号波形を示す図である。

【図４】ＩＣカードチップのウォームリセット時の信号波形を示す図である。

【図５】ＩＣカードチップのＩＣカードコマンド処理時の信号波形を示す図である。

【図６】ＩＣカードチップの非活性化時の信号波形を示す図である。

【図７】ホスト機器によるＭＭＣへのアクセスを示したフローチャートである。

【図８】ＩＣカード制御パラメータとそれに対応するＩＣカードへの処理内容を示す表である。

【図９】ＩＣカードチップに対する第１次ＩＣカード初期化の詳細なフローチャートである。

【図１０】ＩＣカードチップに対する第２次ＩＣカード初期化の詳細なフローチャートである。

【図１１】非活性状態のＩＣカードチップに対するＩＣカード初期化時の信号波形を示す図である。

41

【図１２】活性状態のＩＣカードチップに対するＩＣカード初期化時の信号波形を示す図である。

【図１３】ＩＣカードチップによるセキュリティ処理の詳細なフローチャートである。

【図１４】セキュリティ処理要求ライトコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。

【図１５】ＩＣカードチップによるセキュリティ処理実行時の信号波形とフラッシュメモリチップアクセスの一例を示す図である。

【図１６】セキュリティ処理結果リードコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。

【図１７】インタフェース直通モードにおけるＭＭＣ外部端子とＩＣカードチップ外部端子の対応関係を示す図である。

【図１８】インタフェース直通モードへ移行する処理とインタフェース直通モードから復帰する処理のフローチャートである。

【図１９】インタフェース直通モードへ移行する処理時の信号波形を示す図である。

【図２０】インタフェース直通モードから復帰する処理時の信号波形を示す図である。

【図２１】フラッシュメモリチップの内部構成を示す図である。

【図２２】本発明を適用したＭＭＣの内部構成を簡単に示す図である。

【図２３】本発明を適用したＭＭＣをコンテンツ配信に応用した例を示す図である。

【図２４】本発明を適用したＳＤカードの内部構成を簡単に示す図である。

【図２５】本発明を適用したメモリースティックの内部構成を簡単に示す図である。

【図２６】本発明のＩＣカードチップの内部構成を示す図である。

42

【図２７】並列に処理できるデータリード処理の流れを示した図である。

【図２８】リードコマンドを並列処理する時のコマンドとデータの流れ、処理を時間軸にそって示した図である。

【図２９】並列に処理できるデータライト処理の流れを示した図である。

【図３０】ライトコマンドを並列処理する時のコマンドとデータの流れ、処理を時間軸にそって示した図である。

【図３１】並列に処理できるデータを転送しないコマンドの処理を示した図である。

【図３２】並列に処理できるデータを転送しないコマンドの実行する時の処理を時間軸にそって示した図である。

【図３３】並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを示した図である。

【図３４】並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。

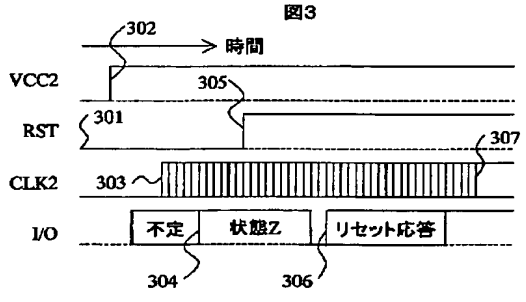
【図３５】並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを示した図である。

【図３６】並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。

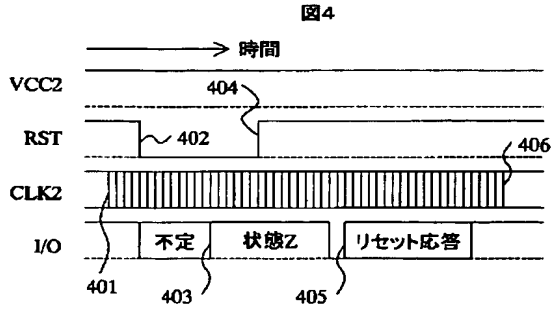
【符号の説明】

１１０…ＭＭＣ、１２０…コントローラチップ、１４０…ＭＭＣ外部端子、１５０…ＩＣカードチップ、１５１…ＶＣＣ２端子、１５２…ＲＳＴ端子、１５３…ＣＬＫ２端子、１５５…ＧＮＤ２端子、１５６…ＶＰＰ端子、１５７…Ｉ／Ｏ端子、２２０…ホスト機器、１４０５…ライトコマンド発行、１９０６…モード移行時刻、２００３…モード復帰時刻。

【図３】

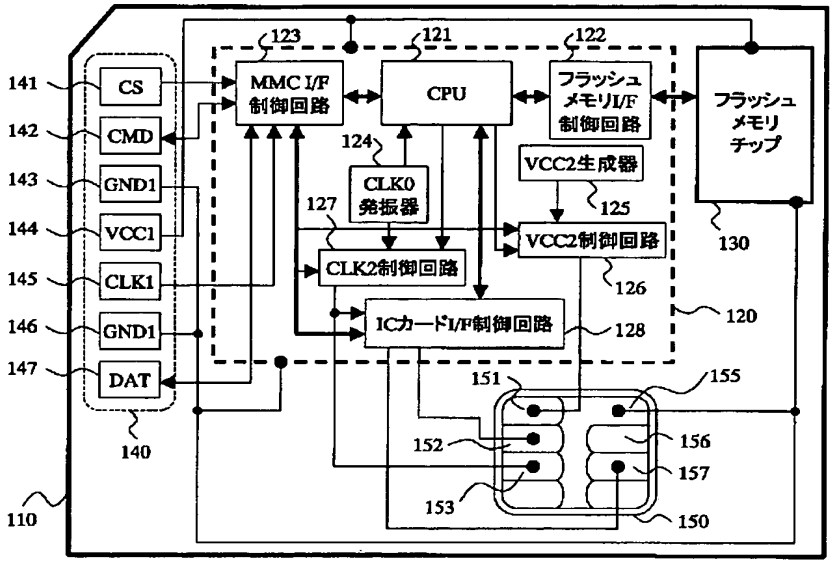


【図４】



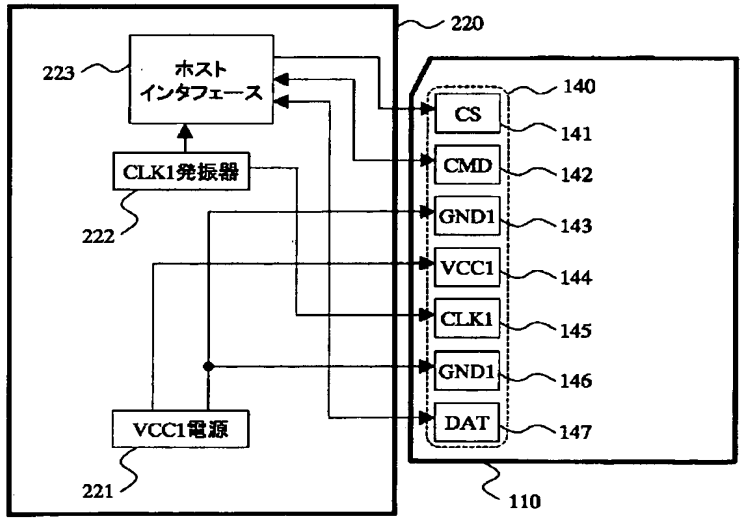
【図１】

図1



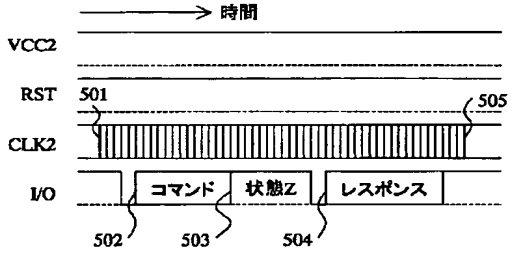
【図２】

図2



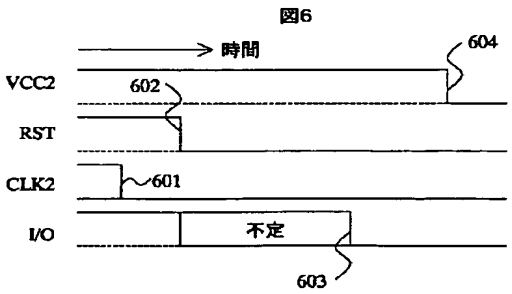
【図５】

図5



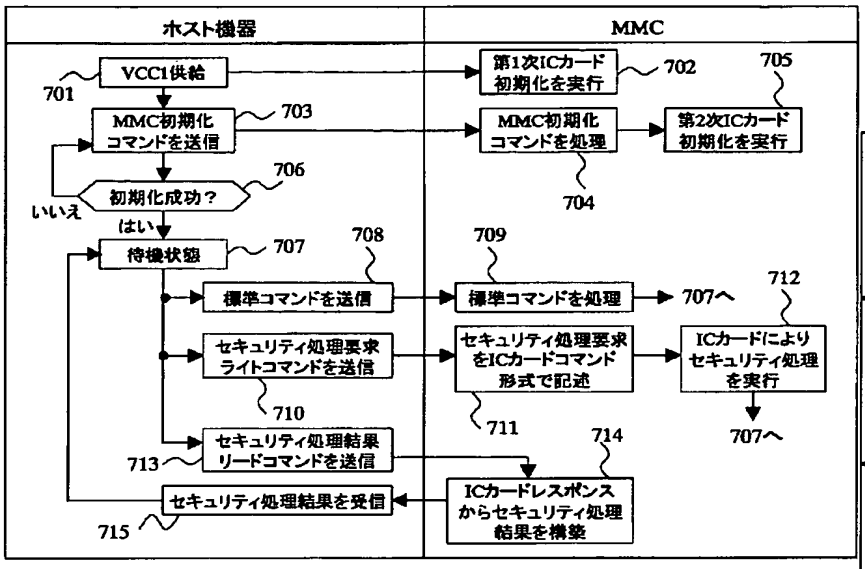
【図６】

図6



【図７】

図7



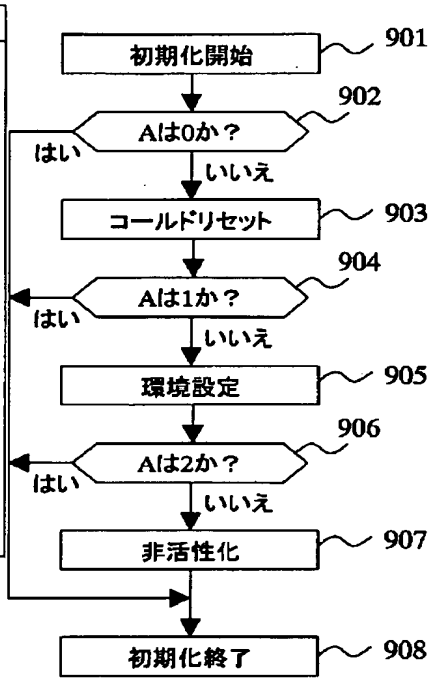
【図８】

図8

ICカード制御パラメータ		ICカードに対する処理
A=0		MMCのパワーオン時に，何もしない
A=1		MMCのパワーオン時に，リセット
A=2		MMCのパワーオン時に，リセットと環境設定
A=3		MMCのパワーオン時に，リセットと環境設定し，非活性化
B=0		MMCの初期化時に，何もしない
B=1	C=1	MMCの初期化時に，リセット
	C=2	MMCの初期化時に，リセットと環境設定
	C=3	MMCの初期化時に，リセットと環境設定し，非活性化
B=2	C=2	MMCの初期化時に，環境設定
	C=3	MMCの初期化時に，環境設定し，非活性化
B=3		MMCの初期化時に，活性状態ならば，非活性化
D=0		セキュリティ処理後に，非活性化しない
D=1		セキュリティ処理後に，非活性化する

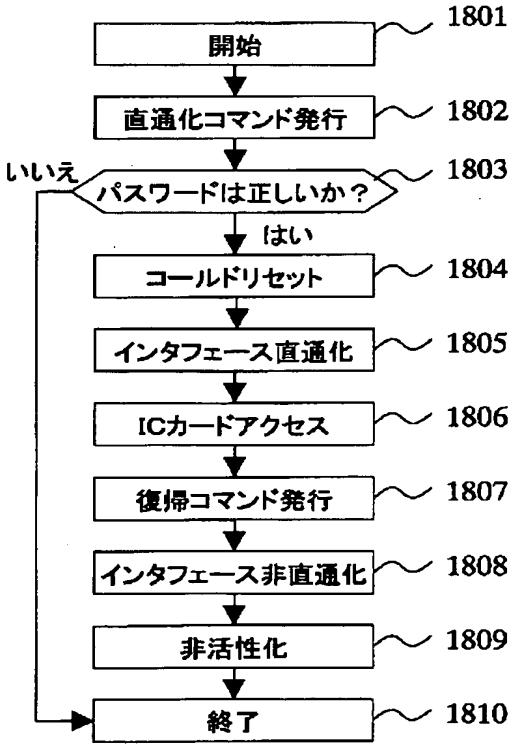
【図９】

図9



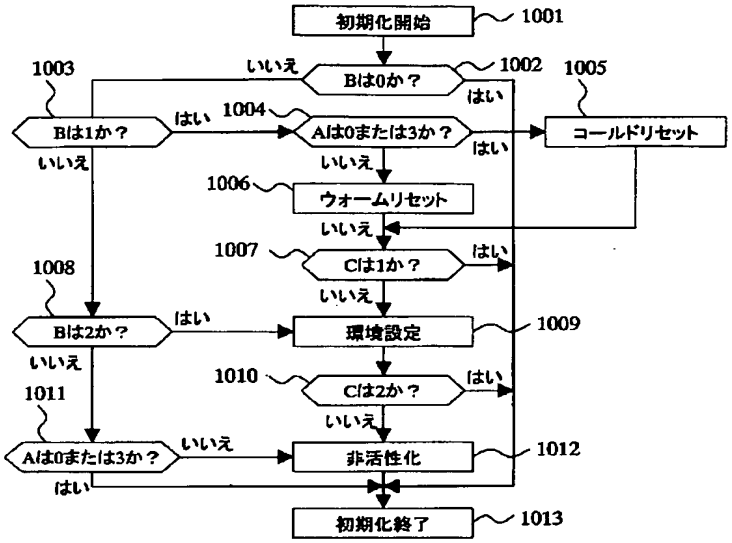
【図１８】

図18



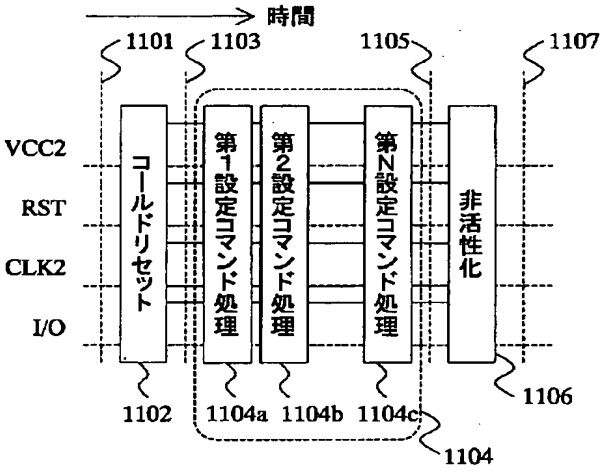
【図１０】

図10



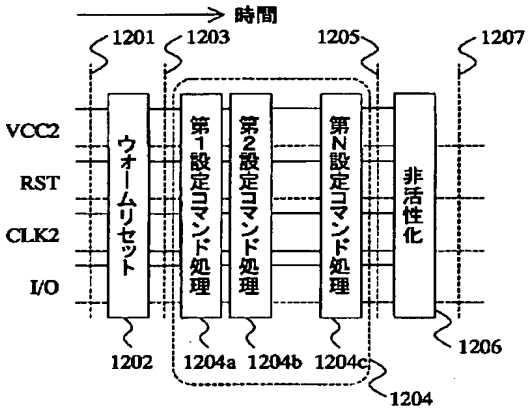
【図１１】

図11



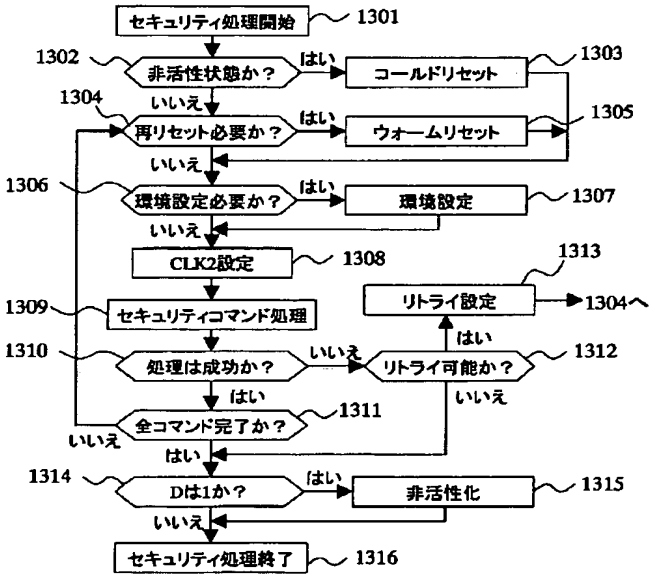
【図１２】

図12



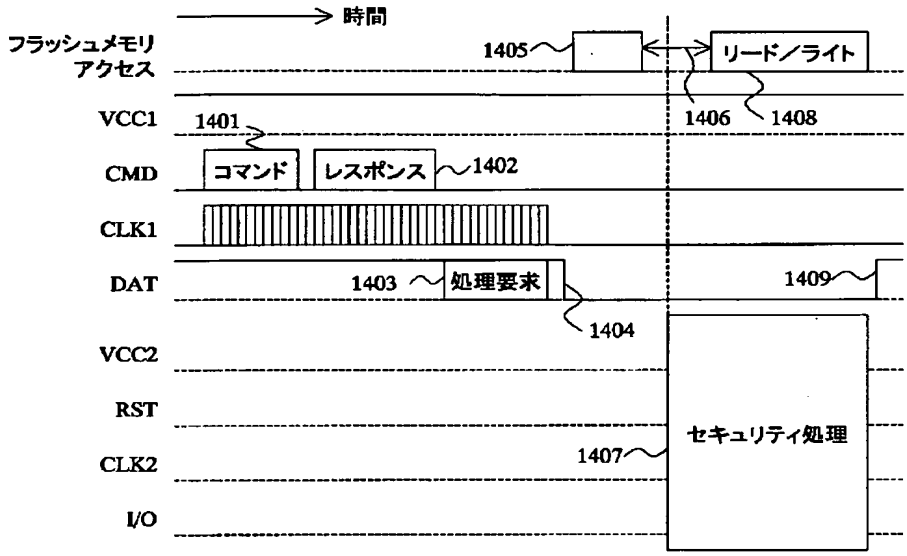
【図１３】

図13



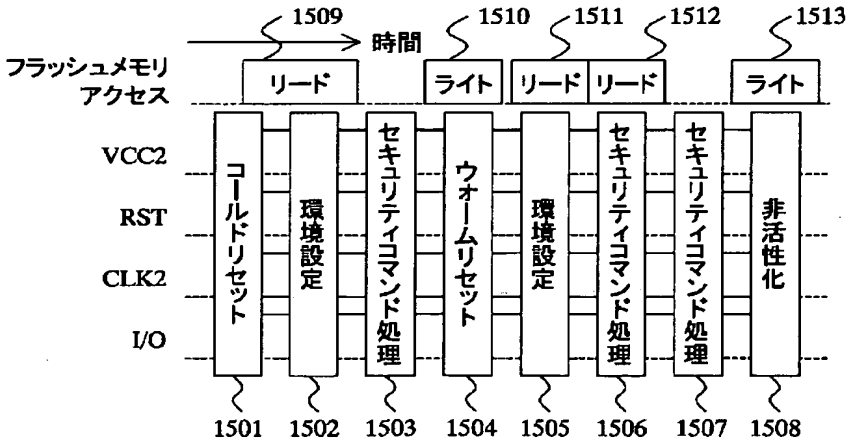
【図１４】

図14



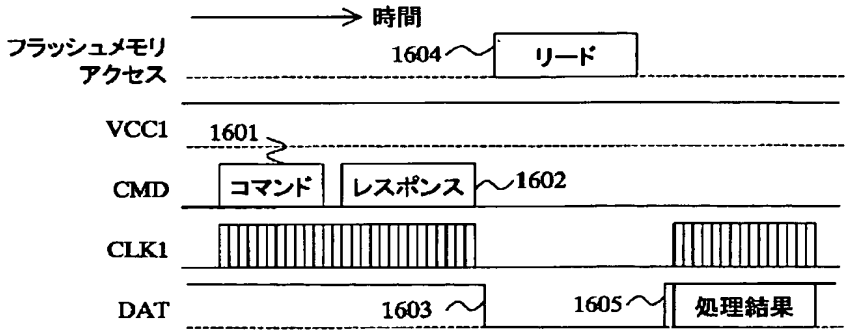
【図１５】

図15



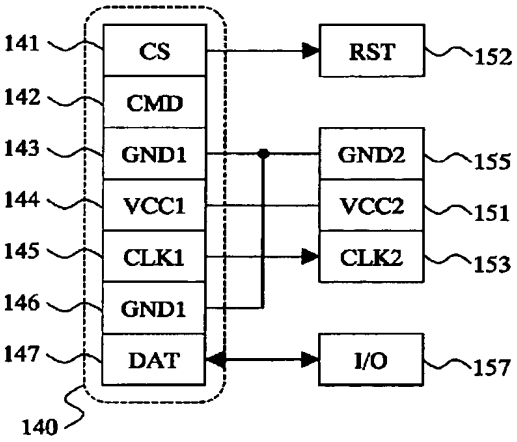
【図１６】

図16



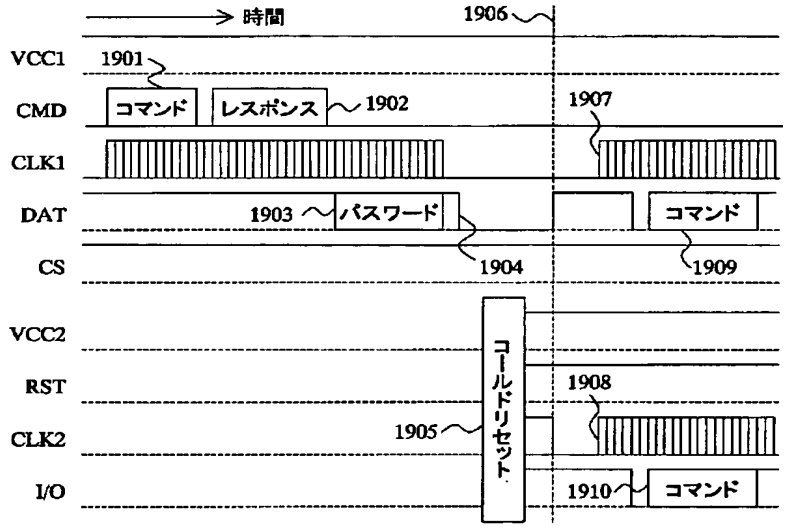
【図１７】

図17



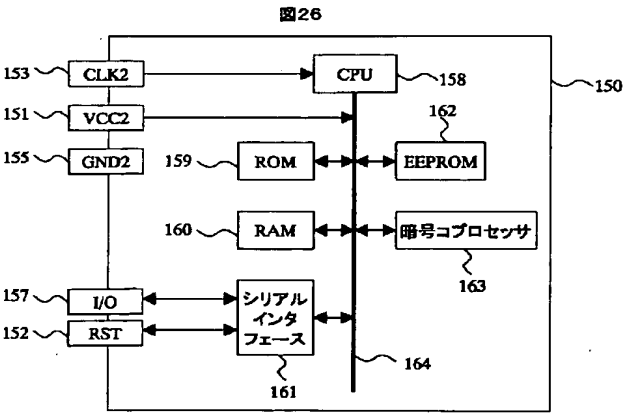
【図１９】

図19



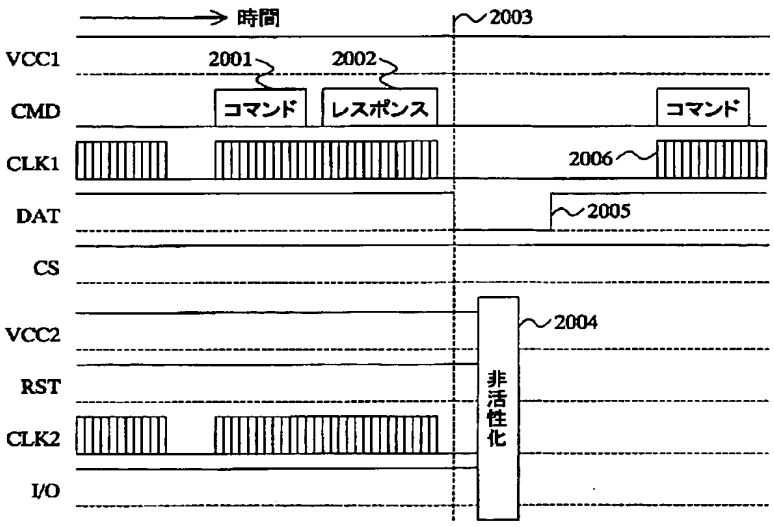
【図２６】

図26



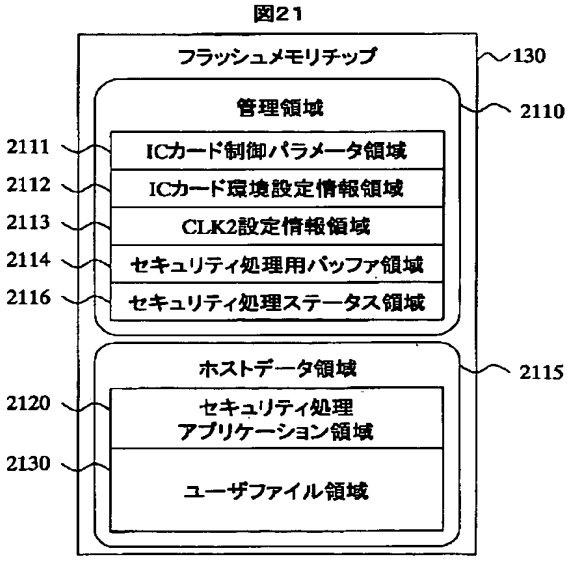
【図２０】

図20



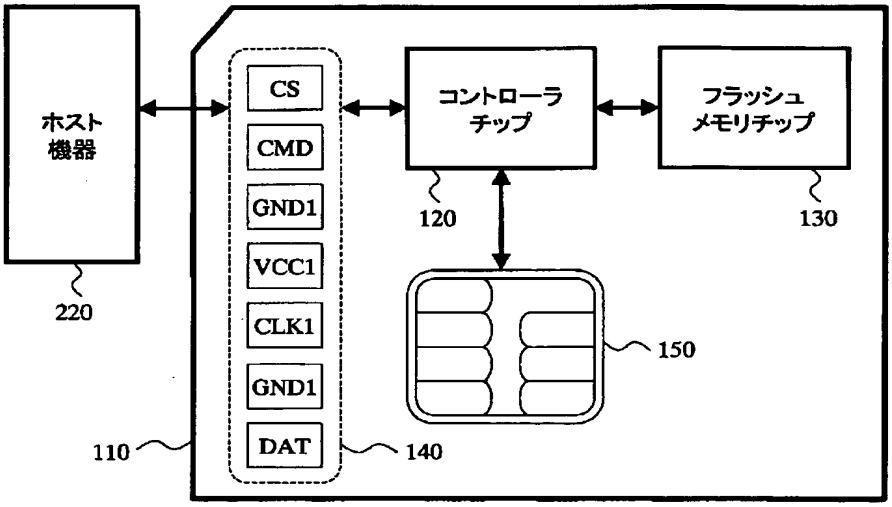
【図２１】

図21



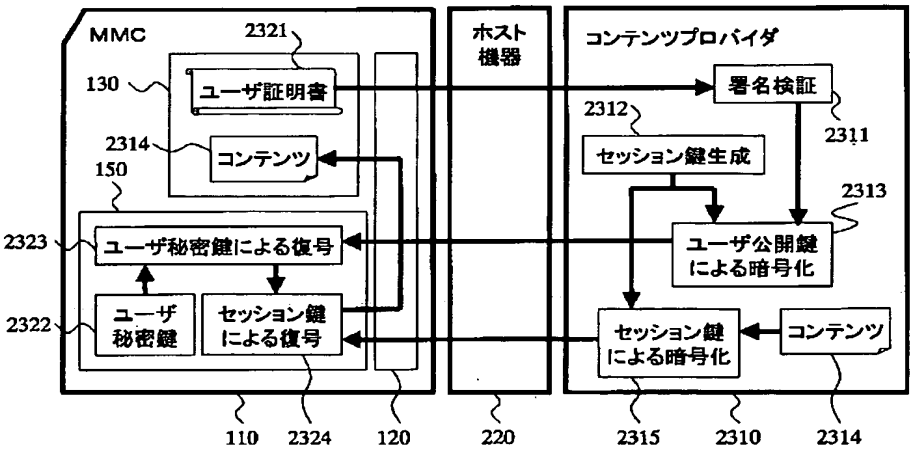
【図２２】

図22



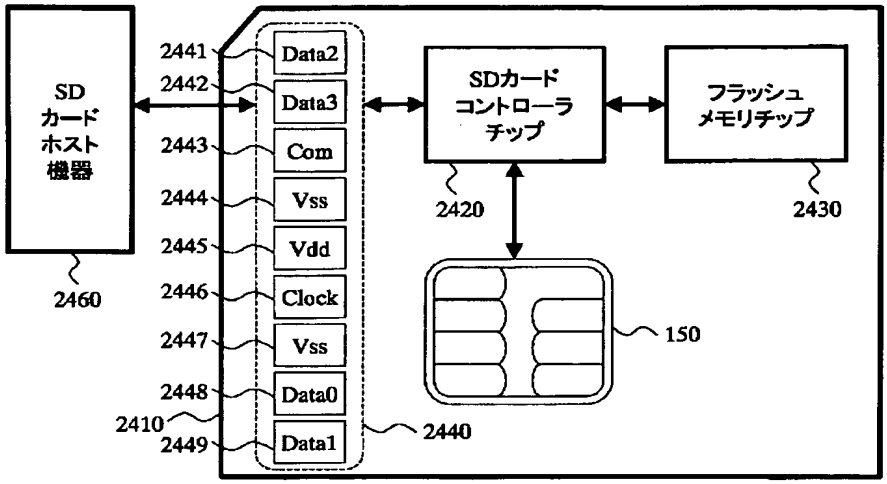
【図２３】

図23



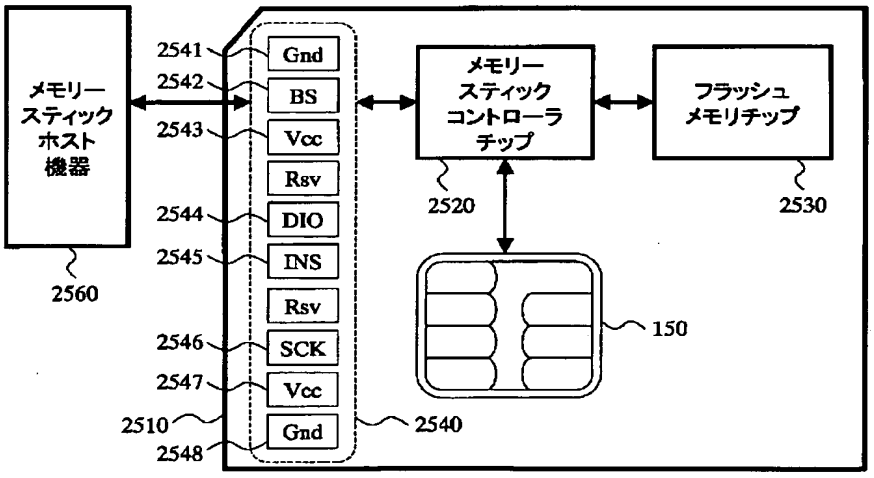
【図２４】

図24



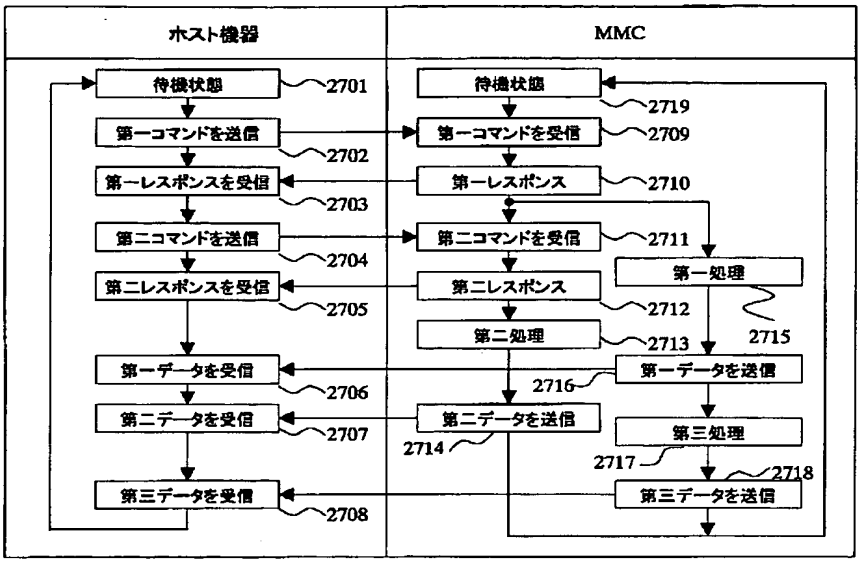
【図２５】

図25



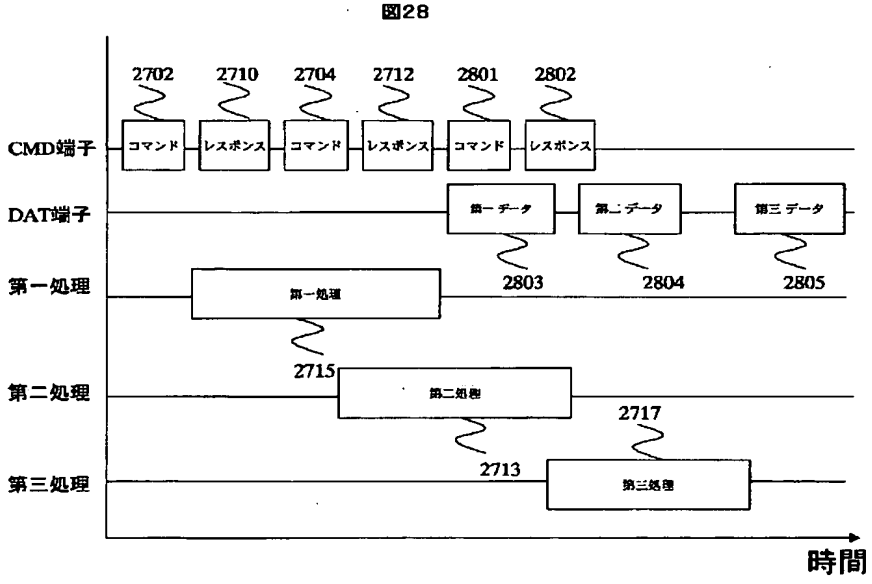
【図２７】

図27



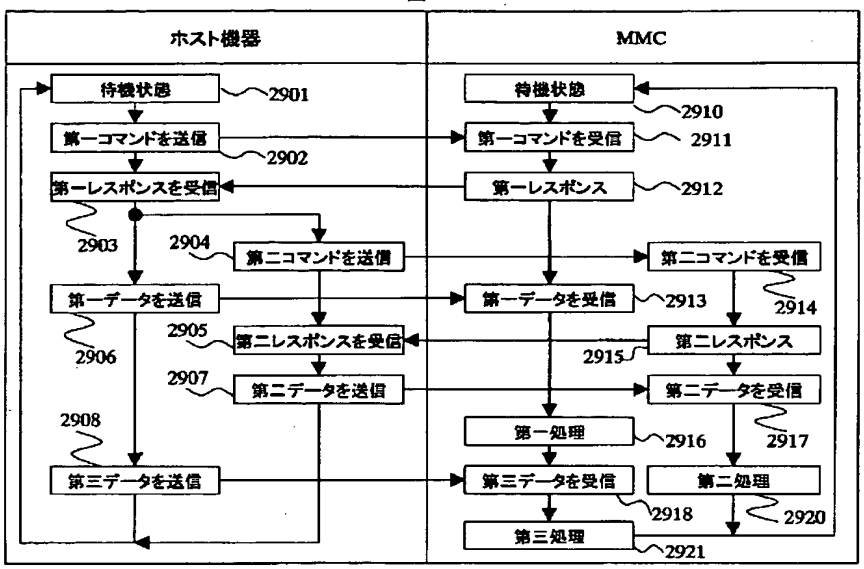
【図２８】

図28



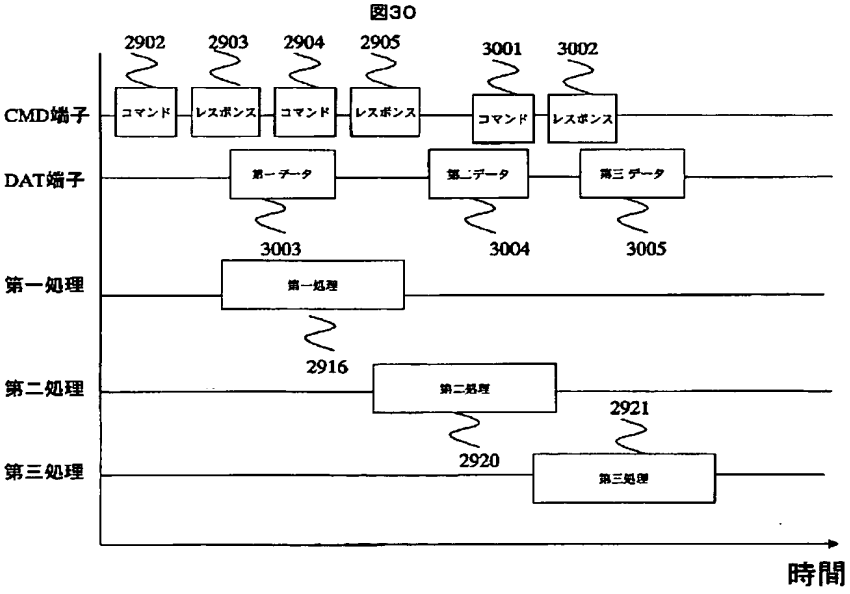
【図２９】

図29



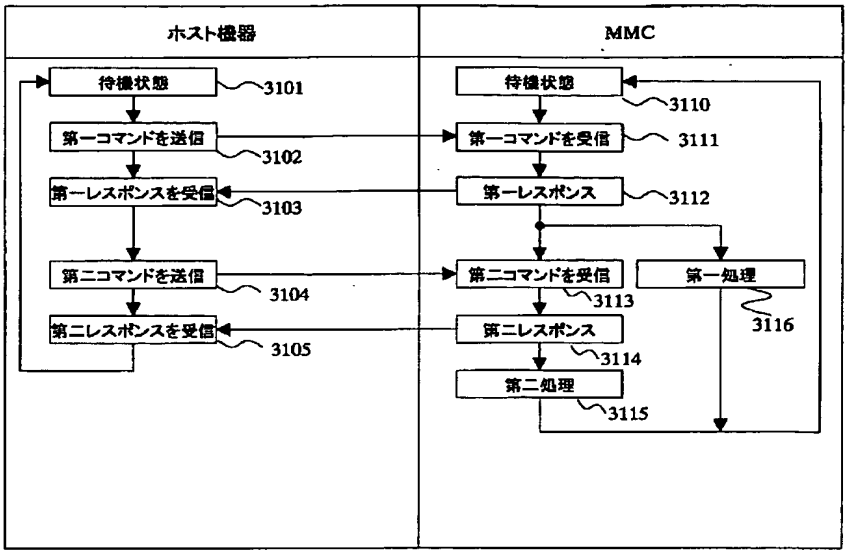
【図３０】

図30



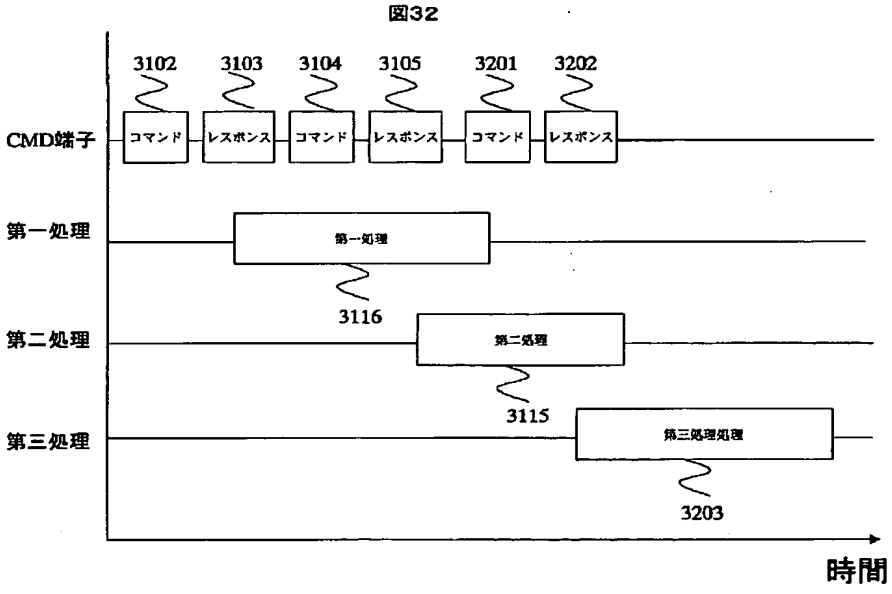
【図３１】

図31



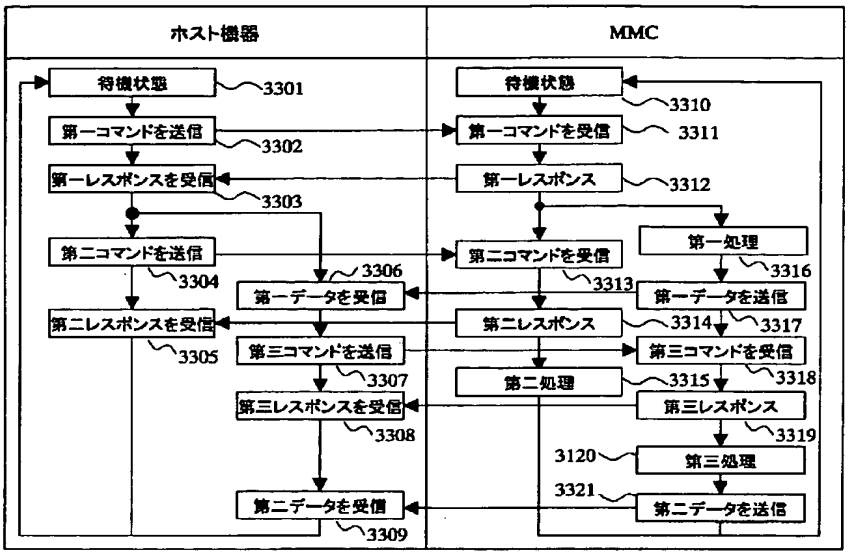
【図３２】

図32



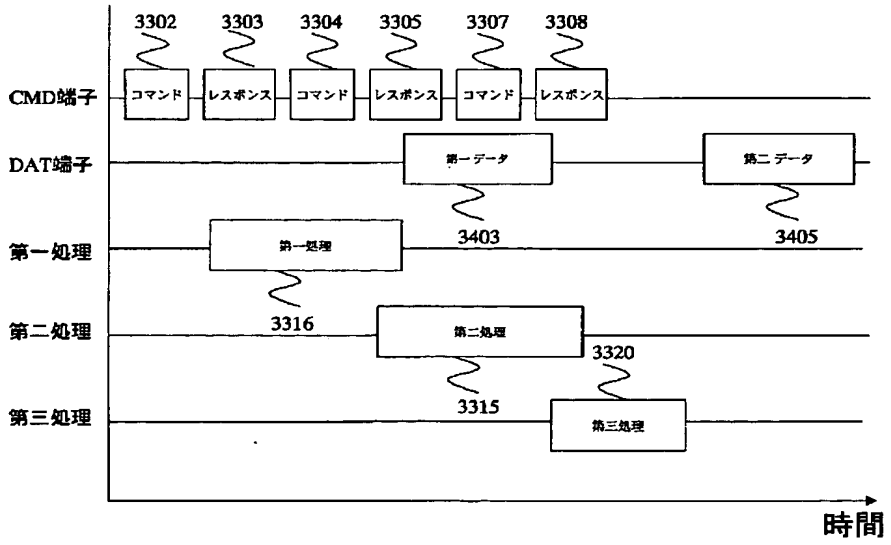
【図３３】

図33



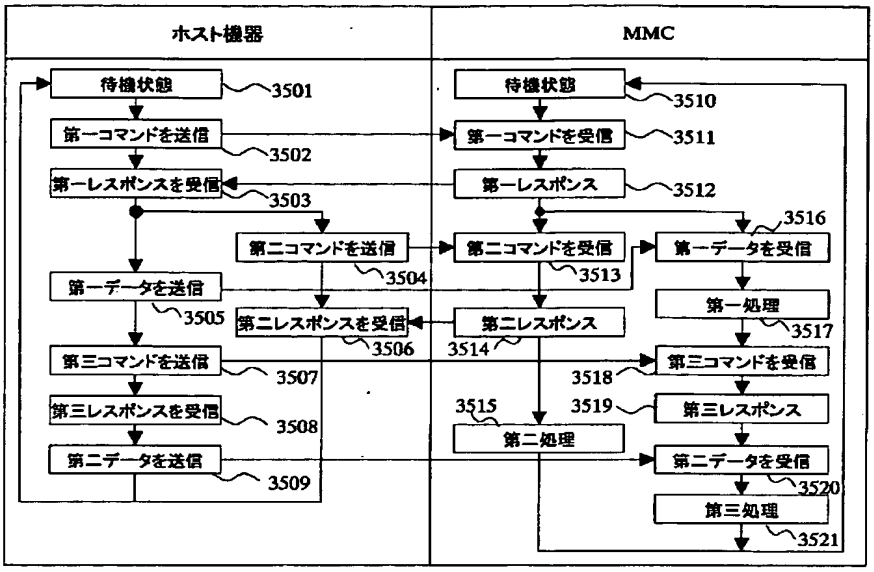
【図３４】

図34



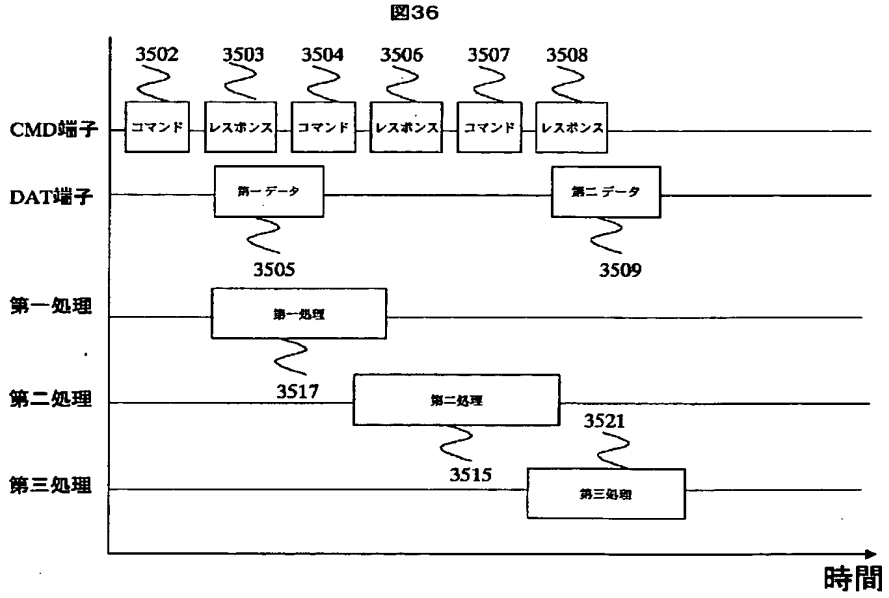
【図３５】

図35



【図３６】

図36



フロントページの続き

(72)発明者　角田　元泰
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　水島　永雅
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　片山　国弘
東京都小平市上水本町五丁目20番１号　株式会社日立製作所半導体グループ内

Ｆターム(参考)　2C005 MA19 MB02 MB07 NA10 PA18
PA21 RA22 WA03 WA09
5B017 AA07 BA06 BA07 CA14
5B035 AA13 BB09 BC00 CA07 CA11
CA29